

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
27 March 2003 (27.03.2003)

PCT

(10) International Publication Number
WO 03/025718 A2

(51) International Patent Classification⁷: G06F 1/00

(21) International Application Number: PCT/GB02/04228

(22) International Filing Date:
17 September 2002 (17.09.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/323,159 18 September 2001 (18.09.2001) US

(71) Applicant: DATA TREASURY CORPORATION
[US/US]; 175 Pinelawn Road, Suite 200, Melville, NY
11747 (US).

(71) Applicant (for MN only): MAGGS, Michael, Norman
[GB/GB]; Kilburn & Strode, 20 Red Lion Street, London
WC1R 4PJ (GB).

(72) Inventors: BALLARD, Claudio R; 16 West Neck Court
Lloyd Harbor, New York, NY 11743 (US). PATHAK,

Amrish; 7 Apple Blossom lane, East Patchogue, New
York, NY 11772 (US). IMBRANCE, Michael T; 291 East
Woodside Avenue, East Patchogue, New York, NY 11772
(US). CURRIE, Edward H; 6-57 158 Street, Whitestone,
New York, NY 11357 (US). CASSATA, James; 673
Meadow Road, Smithtown, New York, 11787 (US).

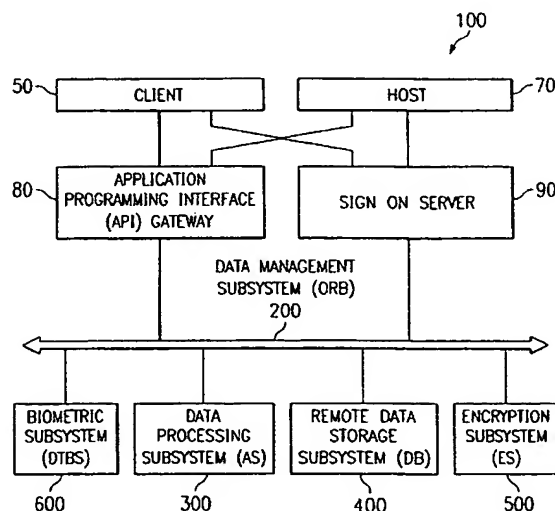
(74) Agents: MAGGS, Michael, Norman_ et al.; Kilburn &
Strode, 20 Red Lion Street, London WC1R 4PJ (GB).

(81) Designated States (national): AE, AG, AL, AM, AT, AU,
AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU,
CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH,
GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC,
LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW,
MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG,
SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC,
VN, YU, ZA, ZM, ZW.

(84) Designated States (regional): ARIPO patent (GH, GM,
KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),
Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),
European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE,
ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK,

[Continued on next page]

(54) Title: BIOMETRICALLY ENABLED PRIVATE SECURE INFORMATION REPOSITORY



(57) Abstract: A system for remote data acquisition and private and secure and authenticated, centralized processing and storage is disclosed called the DataTreasury™ Repository System. The DataTreasury™ Repository System provides a secure system for the storage and retrieval of data comprising personal information, financial information, and general information. The identity of the users are held private through the use of a biometric as the sole personal identifier. The system acquires transactional data at least one remote locations, encrypts the data, transmits the encrypted data to a central location, transforms the data to a usable form, performs identification verification using biometric data, generates informative reports from the data and transmits the informative reports to the remote location(s), while maintaining privacy, security, and authenticity of the user's data and biometric. To ensure the complete security of the system, all data is re-encrypted while in storage, or when it is in a state of nonuse.

WO 03/025718 A2



TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:

— *without international search report and to be republished upon receipt of that report*

BIOMETRICALLY ENABLED PRIVATE SECURE INFORMATION REPOSITORY

* * * * *

BACKGROUND OF THE INVENTION

This invention relates generally to a private system to store and retrieve all types of information with the use of biometrics for authentication and encryption techniques for security.

In this age of the information highway, virtually all personal and financial information is stored within computer systems. Yet this information tends to be scattered among different organizations, like: Federal and local government, bank, merchant, and educational facilities. For this reason, access to all stored information from one source is virtually impossible, or, at the very least impracticable. Furthermore, in certain cases access to information requested by its provider, or owner, is restricted.

In today's information age, users are required to provide personal information freely, however, their access to that information may be strictly prohibited. Merchants normally require financial information to complete transactions, yet they are unlikely to divulge any credit data regarding that individual. Governmental agencies usually maintain a detailed profile database on all individuals, but some, or all, of this information is not accessible to the respective individuals. However, when governmental agencies do allow people to access their information, these venues can be described as inconvenient, limited in accessible hours, entailing waiting on long lines, and inadequate service. These facilities may include: county courthouses, departments of motor vehicles, departments of welfare services, departments of housing, departments of immigration and naturalization services, and the various other government agencies. A major reason the government will not allow computer access to personal information is due to security and identity verification issues. The infeasibility of a secure solution has made convenient access impracticable.

There is not one entity currently available to house all personal information for convenient retrieval. Personal information may include, but is not limited to: leases, deeds, passports, birth certificates, wills, trusts, driver's licenses, bank account information, credit information, commercial transaction information, educational information, and citizenship information.

Even if a secure system was were available, security issues would make people hesitant to supply their personal information electronically. Hackers may attempt to compromise computer systems to conduct vandalism, espionage, and theft. It is possible for hackers to gain successful, unauthorized access to computer systems.

Even for systems with nearly absolute security, by allowing access only to authorized individuals, there is still the danger of fraud through the impersonation of an authorized user. For example, bad checks are abundant within the stream of commerce. Individuals may steal checks and forge signatures.

Other computer systems designs do not reflect the issue of security as a primary concern. Some systems utilize passwords in the form of alphanumeric characters, which can be easily guessed using algorithms capable of generating random combinations of numbers and letters. This type of security is further susceptible to user negligence, e.g., forgotten, lost, stolen, or intercepted passwords.

Other approaches have focused on providing secure identification and verification. U.S. Pat. No. 5,790,668 discloses system and method to provide secure handling of data through means of a personal identifier database. Similarly, U.S. Pat. No. 5,930,804 discloses an invention to provide improved Web-based security measures, and methods to implement such measures and, moreover, to provide improved Web-based authentication systems and methods. Similarly, U.S. Pat. No. 5,870,723 discloses a method and system to provide a biometric transaction authorization with the use of a PIN number. Similarly, U.S. Pat. No. 5,995,630 discloses a method to facilitate secure and authorized access to a computer.

While these approaches provide a method to avoid the problems associated with unauthorized access with user identification, they have disadvantages. These approaches focus

on a gateway comprising security and user verification. First, these approaches do not offer a secure, authenticated centralized repository system. The database element in these approaches is limited to storing information pertinent to a particular business, or security purpose. For example, the databases in these inventions house only biometric information, personal identifiers, limited financial information, or encryption keys. Accordingly, these approaches do not offer an implementable system that serves as a secure repository in which to store any and all types of data.

These approaches also have a security deficiency, as they require a personal PIN number or personal identifier. These methods seriously compromise the security of the system as a whole. PIN numbers can be forgotten, lost, misplaced, and obtained through disreputable algorithmic approaches or other schemes.

Furthermore, systems that require personal identifiers, commonly associate the person's social security number with their identity. These approaches inherently lack the ability to provide anonymity to the users. Information is inexplicably tied to a particular person. Individuals are uniquely identified with ease through a social security number. Moreover, social security numbers are easily accessible and widely utilized. It is common practice for governmental institutions, financial institutions, educational institutions, and medical institutions and to use social security numbers as personal identifiers. Most of these institutions utilize and display social security numbers with disregard for privacy or security. Thus, the identity of the data owner can be easily obtained through his social security number.

However, none of these verification systems offer a general, centralized database to store any, and all, types of data and information. Accordingly, there is a need for a system where any type of information may be stored securely and retrieved with anonymity, ease and convenience. Further, there is a need for a single, comprehensive, information storage system having reliability, privacy, authenticity, and accessibility.

By way of further background, U. S. Patent No. 6,032,137 and U.S. Patent No. 5,910,988 commonly assigned herewith and incorporated herein by this reference, describe data repository systems and methods, for example as applied to commercial payments and transactions.

SUMMARY OF THE INVENTION

This invention involves the storage and retrieval of data with the full identification and verification of users through means of a biometric identifier. The biometric identifier identifies biometric data or biometrics that comprises a statistical analysis of biological data, for example: retina geometry prints, facial prints, DNA data, fingerprints, or voice patterns. Biometric data represents a unique personal identity marker, which is in possession of the user at all times. The use of biometrics ensures a private system due to its inherent characteristics. The DataTreasury™ Repository System uses a biometric, as a unique identity marker. The usage of biometrics effectuates creates an extremely secure method of authentication for access to data stores. Furthermore, as communication protocols have become increasingly sophisticated users can access data anywhere in the world.

Users who wish to enroll into the DataTreasury™ Repository System must first present documents to authenticate their claimed identity. Upon registration they must input their biometrics, and any required information into client stations. The biometrics obtained through the registration process are stored in an enrollment biometric database. The enrollment biometrics are utilized to assist in the verification of the user in future transactions.

As a paradigm, merchants, as well as financial institutions, may enroll in to the DataTreasury™ Repository System to facilitate financial transactions. Commercial users can take the form of a host within the DataTreasury™ Repository System, and utilize its services to conduct business. Financial transactions are not limited to financial institutions, which are enrolled into the system. The DataTreasury™ Repository System may further communicate, transmit information, facilitate transactions with financial institutions, which are not enrolled. The DataTreasury™ Repository System may further communicate, and conduct transactions with any non-enrolled user, entity, whether an institution, a business, or an individual.

It is an object of the present invention to provide a system for a secure, centralized storage of all types of information. For example, a system which could handle commercial

transaction information, financial information, credit information, citizenship information, educational information with authenticated access, would comprise:

- at least one remote client subsystem designed to receive and transmit data;
- at least one remote data processing subsystem designed to facilitate the processing of data, comprising an encryption subsystem to ensure a secure, biometric authentication subsystem to ensure the identity of users;
- at least one remote data management subsystem to manage the processing of data;
- at least one remote data storage subsystem to store any, and all, types of data;
- and
- at least one communication network for secure transmission of data within, and between the data processing subsystem, the data management subsystem, and the data storage subsystem.

The DataTreasury™ Repository system securely supplies authenticated access to information such as, credit information, banking information, personal information, real-estate information, employment information, and commercial transaction information.

It is a further object of the DataTreasury™ Repository System to facilitate: private and secure financial transactions, via a centralized, secure, and easily accessible system worldwide.

It is a further object of the DataTreasury™ Repository System to facilitate a virtually fraud proof system of conducting transactions.

It is a further object of the DataTreasury™ Repository System to facilitate a private method to traverse the internet.

It is a further object of the DataTreasury™ Repository System to facilitate the secure and private electronic communication between computer systems.

It is a further object of the DataTreasury™ Repository System to facilitate the registration process for warranties, and similar legal documents.

It is a further object of the DataTreasury™ Repository System to secure email communication and prevent unsolicited advertisements or spamming.

It is further object of the DataTreasury™ Repository System of the invention to store and provide data with a multi-tiered architecture comprised of the DataTreasury™ Object Request broker (ORB), the DataTreasury™ Application Server (AS), the DataTreasury™ Database (DB), DataTreasury™ Encryption Subsystem (ES), and a DataTreasury™ Biometric Subsystem (DTBS).

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING

These and other objects and features of the invention will be more clearly understood from the following detailed description along with the accompanying drawing figures, wherein:

FIG. 1 is a block diagram of the DataTreasury™ Repository System (DRS) architecture;

FIG. 2 is a block diagram of the distributed environment;

FIG. 3 is a block diagram of the client subsystem;

FIG. 4 is a block diagram of the Object Request Broker (ORB) architecture;

FIG. 5 is a block diagram of the Application Server (AS) architecture;

FIG. 6 is a block diagram of the Encryption Server architecture;

FIG. 7 is a block diagram of the process for analyzing and storing biometrics using the DataTreasury™ Biometric Subsystem architecture;

FIG. 8 is a block diagram of the communication network;

FIG. 9 is a flow chart of the process for transferring information;

FIG. 10 is a flow chart describing the process for the DRS; and

FIG. 11 is a flow chart of the second embodiment of the process shown in FIG. 9.

DETAILED DESCRIPTION OF THE INVENTION

Fig. 1 displays the block diagram of a DataTreasury™ Repository System (DRS) 100, which is connected to either clients 50 or hosts 70 via either an Application Programmable Interface (API) gateway 80 or through a sign on server (SOS) 90. The DataTreasury™ Repository System 100 has five elements: a DataTreasury™ Object Request broker (ORB) 200 (transaction management subsystem), a DataTreasury™ Application Server (AS) 300 (data processing subsystem), a DataTreasury™ Database (DB) 400 (data storage subsystem), DataTreasury™ Encryption Subsystem (ES) 500 (system to ensure security), and a DataTreasury™ Biometric Subsystem (DTBS) 600 (system to process and verify biometrics).

As shown in FIG. 2, the DataTreasury™ Repository System 100 uses an object oriented programming language for housing any and all types of information across a distributed environment. Data is sent to the ORB 200 via client subsystems 50 and hosts 70. This information is first encapsulated, next, it is compressed and then it is encrypted before it is sent through API gateway 80 or SOS 90. This information is then decrypted and processed through ORB 200, which in connection with AS 300 ES 500 and DTBS 600, processes this information. This information is then sent on to DB 400 for storage of this information or retrieval of additional information stored in DB 400. A communication network 800 connects these elements together. As shown, API gateway 80 SOS 90, ORB 200, AS 300, DB 400, relational databases 430, ES 500, and DTB 600 are all housed in a central location. API gateway 80 or SOS 90 are designed to receive information from clients 50 or hosts 70. SOS 90 is designed as a single sign on server whereby with one password or one set of biometric information, the user can gain access to multiple accounts that would formerly take multiple login identifications and passwords.

Client subsystem 50 is shown in greater detail in FIG. 3, ORB 200 is shown in greater detail in FIG. 4, AS 300 is shown in greater detail in FIG. 5, ES 500 is shown in greater detail in FIG. 6, the process for DTBS 600 is shown in greater detail in FIG. 7, and communication network 800 is shown in greater detail in FIG. 8.

As shown in FIG. 3, client subsystem 50 provides a convenient interface to users to enable data entry and extraction from the DB 400. A simplified interface to enable data extraction from a database for use in the present invention is described in United States Patent No. 5,910,988, United States Patent No. 6,032,137, and United States Patent Application 09/454,492 to Ballard, entitled "Remote Image Capture with Centralized Processing and Storage", which is incorporated herein by reference. Furthermore, the client subsystems 50 may also be hosts 70. These client subsystems may contain a biometric processing client subsystem 51, and a data capturing device 53. The client subsystem may contain input devices 55 such as but not limited to: video cameras, digital cameras, CD-ROM readers, DVD readers, keyboards, mice, microphones, smart card readers, scanners, magnetic strip readers, MICR readers, 2D/3D bar code readers, and biometric capture devices. The client subsystem may also contain output devices 57 which may facilitate report generation such as but not limited to: monitors, printers, and speakers. Client subsystems 50 may further take any form comprising a point of sale, Internet, or wireless machines, to name a few. Furthermore, client subsystems 50 may also contain a biometric device 59 for capturing biometric data.

Client subsystems 50 may connect to the ORB 200 through a communication network such as communication network 800. However client subsystem 50 may connect to ORB 200 by any means including, but not limited to, the internet, wireless RF, microwave, infrared or, through a wired local or wide area network. A wireless data network may be used for connecting one or more client subsystems 50 to one or more centralized processing facilities, this wireless network is employed for either local area network (LAN) or wide area network (WAN) connectivity, or both simultaneously. The wireless network is not limited to a specific technology, transmission speed, or mode of operation. The physical means for communication between the client subsystem 50 and the ORB 200 may be facilitated by, but not limited to modems, cables, fiber optics, or satellites. Furthermore, Client subsystems 50 are not tied to a specific programming language. Client subsystems 50 and AS 300 in a distributed environment need only communicate in terms of the ORB 200, interface. The ORB 200 may act as a middleware layer between the client subsystems 50 and all types of heterogeneous sources. Furthermore, the ORB 200 may automate services such as, but not limited to: object registration, location, activation, and demultiplexing. The ORB 200 handles the request between the client

subsystem 50 to the AS 300. Objects 350 are encapsulated packages of code and data that can be manipulated by operations through a defined interface. The ORB 200 initiates queries of the DB 400, which are necessary for object 350 functionalities. An essential aspect of the DataTreasury™ Repository System is that it enables, identifies, authenticates, and processes information using, inter alia, biometric and cryptographic algorithms.

As is known to persons of ordinary skill in the art, the DataTreasury™ Repository System 100 could also use other software development standards, other system deployment standards, and other reliability standards as long as adherence to these alternative standards provides the security, availability, integrity and reliability required by mission critical applications of this scale. See, e.g. Fayad, Johnson, and Schmidt, "Building Application Frameworks: Object Oriented Foundations of Framework Design", chap. 1 to chap. 6, (Wiley, 1999)

Fig. 4 is a block diagram of the ORB 200 architecture. ORB 200 can exist on one or more servers and can contain a transaction processing architecture 250, which manages objects 230 such as application objects 232, domain objects 234, and database objects 236. In addition, transaction processing architecture 250 also manages events 255, transactions 265, persistence 270, concurrency 275 and security 260. In the preferred embodiment, the ORB 200 is facilitated through the use of Common Object Request Broker Architecture (CORBA). The ORB 200 may provide a series of services including but not limited to: life cycle services, persistence services, naming services, event services, concurrency control services, transaction services, relationship services, externalization services, query services, licensing services, and properties services. Life cycle services define how to create, copy, move, and delete components. A component is a reusable program building block that can be combined with other components in the same or other computers in a distributed network to form an application. The persistence service facilitates the ability to store data on the DB 400.

The naming service allows components to find other components by name. The event service allows the components to specify specific events to be notified of. The concurrency control service allows the ORB 200 to manage locks to data caused by competing transactions or threads. The transaction service ensures that once transactions are completed, the required

functions are performed, and to ensure the consistency of the DB 400. The relationship service can create and/or keep track of dynamic associations between components. The externalization service provides a method to add and obtain data from a component resident in a stream of data. The query service allows the component to query the DB 400. The licensing service allows the use of the component to be measured. Lastly, the properties service allows components to have a self description, which in turn can be used by other components. The client subsystems 50 use stubs to invoke the required application objects 230 in AS 300 through the ORB 200 for the required transaction. ORB 200 can also contain a memory hierarchy 262 containing a primary memory 264 and a secondary memory 266.

In the preferred embodiment, the ORB 200 server comprises stand-alone IBM Enterprise RS/6000 7026 Model M80 servers, which are connected through a common network. Typically, the IBM Enterprise RS/6000 7026 Model M80 class computers have 6 GB of RAM, a 1.26 TB Shark storage array, and gigabit Ethernet network connection.

The client subsystems 50 requests to the AS 300, DB 400, ORB 200, and hosts 70 are facilitated through CORBA compliant services. Object request brokers, ORB 200 can create a persistent link between client subsystems 50, hosts 70 and AS 300 for servicing requests. AS 300 and ORB 200 are usually the middle tier and databases are maintained in the third tier. AS 300 requires CORBA services to communicate with third tier databases for executing queries.

As is known to persons of ordinary skill in the art, CORBA or any equivalent architectural framework may be utilized to construct an ORB 200 to provide load balancing and allocation of services between application servers and databases.

In an alternate embodiment, an information gateway may be utilized to construct the ORB 200. The object based ORB 200 may be also implemented with a message, transaction, or event based architectural frameworks. An exemplary embodiment of alternate architectural frameworks which may be utilized, as known to persons of ordinary skill in the art, include but are not limited to: MQ series, Tuxedo, and Rendezvous. See, e.g., Bernstein, and Newcomer, "Principles of Transaction Processing", chap. 2 to chap. 10, (Morgan Kaufman Publishers, 1997). Additionally, see, e.g., Primates, "Tuxedo, an Open Approach to OLTP", chap. 2 to chap. 6,

(Prentice Hall, 1995). Further, see, e.g., Gilman and Schreiber, "Distributed Computing with IBM MQSeries", chap. 3 to chap 10, (Wiley, John & Sons, Incorporated, 1996).

As will be understood by those skilled in the art, Object-Oriented Programming (OOP) techniques involve the declaration, definition, creation, invocation and destruction of "objects" 230. OOP focuses on objects rather than specific functions. In object-oriented programming, objects are the concepts to consider first in designing a program and they may also comprise units of code that are eventually derived from the process. In between, each object is made into a generic class of object and even more generic classes are defined so that objects can share models and reuse the class definitions in their code. Each object is an instance of a particular class or subclass with the class's own method or procedures and data variable. An object is what actually runs in the system. See, e.g., Rumbaugh, Blaha, Premerlani, Eddy, and Lorensen, "Object Oriented Modeling and Design", chap. 1 to chap. 10, (Prentice Hall, 1991). These objects 230 are software entities comprising data elements and routines, or functions, which manipulate the data elements. The data and related functions are treated by the software as an entity and can be created, used and deleted in a parallel and concurrent fashion. Together, the data and functions enable objects 230 to model virtually any real-world entity in terms of its characteristics, represented by the data elements, relationships and its behavior. Object 230's behavior determines how and when it manipulates its data elements. In this way, objects 230 can model complex physical phenomena like weather systems, and it can also model abstract complexities like many mathematical algorithms.

In the preferred embodiment, through a communication network, the ORB 200 are connected to the AS 300 and DB 400 through a LAN using switched 1000BaseT/100BaseT Ethernet, using TCP/IP protocol, though the invention is not so limited. As is known to persons of ordinary skill in the art, the 1000BaseT/100BaseT Ethernet is a networking link layer protocol. Further, the numbers 1000 and 100 refer to the communication link speed in megabits per second. In the preferred embodiment the CISCO Catalyst 6000, model No. 6509, Network Switch or equivalent hardware supports the LAN connectivity between the devices connected to it. A communication network for use in the present invention is described in United States Patent No. 5,910,988, United States Patent No. 6,032,137, and United States Patent Application

09/454,492 to Ballard, entitled "Remote Image Capture with Centralized Processing and Storage", which is incorporated herein by reference.

The ORB 200 and the client subsystems 50 are connected on a Wide Area Network (WAN). A WAN router facilitates communication between the client subsystem 50 and the ORB 200. In the preferred embodiment, the WAN uses frame relay connectivity. As is known to persons of ordinary skill in the art, frame relay is a network protocol for data communication. In contrast to dedicated point-to-point links that provide a fixed data rate, frame relay communication provides variable bandwidth availability on-demand with a guaranteed minimum data rate. Frame relay communication also allows occasional short high data rate bursts according to network availability. In the preferred embodiment, the CISCO 2621 router, or equivalent hardware, supports the WAN connectivity between the devices.

Each frame encloses one user packet and adds addressing and verification information. Frame relay data communication typically has transmission rates between 56 kilobytes per second (kb/s) and 1.544 megabytes per second (Mb/s). Frames may vary in length up to a design limit of approximately 1024 bytes.

In the preferred embodiment, the telecommunications frame relay carrier cloud is a communication network, which receives the frames destined for the ORB 200 sent by the WAN router from the client subsystems 50. As is known to persons of ordinary skill in the art, carriers provide communication services through local central offices. These central offices contain networking facilities and equipment to interconnect telephone and data communications to other central offices within its own network and within networks of other carriers.

Since the component links of the interconnection network are shared by the carrier clients, data communication must be dynamically assigned to links in the network according to availability. Because of the dynamic nature of the data routing, the interconnection network is referred to as a carrier cloud of communication bandwidth.

The ORB 200 may be coupled with a firewall (See FIG. 6) to provide more secure communication. A firewall is a security device which prevents unauthorized users and/or data traffic from gaining access to a computer network, and/or monitors the transfer of information

to and from the network. Client subsystem 50 requests and system responses between system and client subsystem 50 programs are communicated through a filtering router. Firewalls are well known within the art. See, e.g., Strebe and Perkins, "Firewalls 24 Seven", part 1 and part 2, (Sybex, Network Press, 2000). Filtering routers interrogate the source and destination addresses of open network messages communicated through the router to verify that the source and destination addresses conform to the requirements specified by the operator for communication through the router.

For example, the filtering router does not pass communication messages through it, when these messages arrive from an external network that have a source address which corresponds to the same network for the destination address. This prevents a "spoofing" attack where a computer outside a computer network attempts to emulate another computer on the network to which the destination address computer is coupled, to exploit potentially lower security measures for computers on the same network. Spoofing is the attempt to exploit the source routing feature of the TCP/IP protocol by intentionally creating packets with incorrect IP addresses. In spoofing the hacker disguises himself as a host 70 or router on the targeted network to circumvent some security measures. Transmission from the ORB 200 is preferably first passed through a proxy firewall. Proxy firewalls require the use of a proxy server, or bastion host. The bastion host prevents the direct access to Internet services by the internal users by acting as their proxy, and filtering out unauthorized traffic. A proxy is a structure, where one system acts as a vanguard to another system in making and responding to request. The firewall is preferably implemented with PGP Security Inc. Gauntlet, version 5.5. This is a fully integrated system which provides both packet filtering and proxy services. It also contains software enabling remote management of the firewall throughout the entire enterprise.

Fig. 5 is a block diagram of the DataTreasury™ Application Server (AS) 300. The AS 300 processes all transactions initiated by the ORB 200. However, it is essential that each transaction must be first verified by the encryption application object subsystem 230 and the biometrics application object subsystem 230. A system for processing data for later authorized retrieval for use in the present invention is described in United States Patent No. 5,910,988, United States Patent No. 6,032,137, and United States Patent Application 09/454,492 to Ballard, entitled

"Remote Image Capture with Centralized Processing and Storage", which is incorporated herein by reference.

In the preferred embodiment, the AS 300 server comprises stand-alone IBM Enterprise RS/6000 7026 Model M80, which are connected on a common network. Typically, the IBM Enterprise RS/6000 7026 Model M80 class computers have an 6 GB of RAM, a 1.26 TB Shark storage array, and a gigabit Ethernet network connection.

Application services of the AS 300 are preferably application programs written in a programming language such as Java, C, or C++. In a preferred embodiment, the invention is implemented in the C++ programming language using object-oriented programming techniques. C++ is a compiled language, that is, programs are written in a human-readable script and the script is then provided to a program called a compiler, which transforms the human readable code and produces object code. The resulting object code is then processed by a second process, called a linker. The linker incorporates various library routines required by the object code. The output of the linker is machine executable code. As described below, the C++ language has certain characteristics which allow a software developer to easily use programs written by others while still providing a great deal of control over the reuse of programs to prevent their destruction or improper use. The C++ language is well known and many articles and texts are available which describe the language in detail. In addition, C++ compilers are commercially available from several vendors including Sun Microsystems, Inc. and Microsoft Corporation. Accordingly, for reasons of clarity, the details of the C++ language and the operation of the C++ compiler will not be discussed further in detail herein.

As used herein, the term "object" refers to an encapsulated package of code and data that can be manipulated by operations through a defined interface associated with a distributed object 350. The encryption subsystem 500, biometric subsystem 600, collector subsystem, and other business application subsystems are all instantiated through AS 300 objects. Thus, distributed objects 350 will be seen by those skilled in the art as including the basic properties that define traditional programming objects. However, distributed objects 350 differ from traditional programming objects by the inclusion of two important features. First, distributed objects 350 are multilingual. Distributed objects 350 may be comparable to object abstractions in

various programming languages. Distributed object 350 provides a set of fields and methods accessible to clients 50. Distributed objects 350 give users a virtual model of the data source, allowing seamless integration of heterogeneous data models and protocols. A framework is necessary for management of the distributed objects. The framework can dynamically replicate objects, providing automatic load balancing, event handling and fault tolerance. This technology offloads business logic processing from the client 50 side onto middleware object services.

The interfaces of distributed objects 350 are defined using an interface definition language that can be mapped to a variety of different programming languages. The Object Management Group produces one such Interface Definition Language (IDL). IDL is a language used by CORBA to define interfaces between application components. The IDL generates the stubs and skeletons.

Second, distributed objects 350 are location, language, client subsystem 50, or hosts 70 independent, i.e., distributed objects 350 can be located anywhere in a network. This contrasts sharply with traditional programming objects, which typically exist in the same physical address space as the client subsystem 50. Distributed objects 350 can be object clients or object servers, depending upon whether the object 350 sends requests to other objects 350 or replies to requests from other objects 350. Requests and replies are made through the ORB 200, which is aware of the locations and status of the objects 350. A distributed object system refers to a system comprising distributed objects 350 that communicate through the ORB 200. An object reference is a unique way to identify objects 350. The creation and definition of object references dependent on the ORB 200 will be familiar to those skilled in the art.

When a client subsystem 50 calls one of the AS 300 objects 350 to invoke an object operation, the corresponding stub points to a skeleton. The ORB 200 passes the invocation from the client subsystem 50 stub to the application server skeleton. Stubs are code produced by the IDL compiler in conjunction with client subsystem 50 applications to facilitate an interface with the ORB 200. Skeletons are proxy code, which facilitates the application server implementations through a corresponding interface. The corresponding object 350 implementation to the

skeleton is then able to perform the requested service; which in turn can return any results through the ORB 200 skeleton to the client subsystem 50.

In the preferred embodiment, through communication network 800, the AS 300 are connected to the ORB 200 using switched 1000BaseT/100BaseT Ethernet, and TCP/IP protocol though the invention is not so limited. As is known to persons of ordinary skill in the art, 1000BaseT/100BaseT Ethernet is a networking link layer protocol. Further, the numbers 1000 and 100 refer to the communication link speed in megabits per second. In the preferred embodiment the CISCO Catalyst 6000, model 6509, Network Switch or equivalent hardware supports the LAN connectivity between the devices connected to it.

Turning back to FIG. 2, there is a block diagram of the DB 400 having associated databases 430. DB 400 is responsible for replication and synchronization and responds to queries directed by the ORB 200. An essential aspect of the DB 400 is its storage and retrieval of any type of data including biometric data. In the preferred embodiment all data stored in the DB 400 is encrypted to maximize privacy and security. A remote secure, reliable, and centralized repository to store data for later retrieval for use in the present invention is described in United States Patent No. 5,910,988, United States Patent No. 6,032,137, and United States Patent Application 09/454,492 to Ballard, entitled "Remote Image Capture with Centralized Processing and Storage", which patent is incorporated herein by this reference.

In the preferred embodiment, the DB 400 server comprises stand-alone IBM Enterprise RS/6000 7026 Model M80 servers, which are connected on a common network. The IBM Enterprise RS/6000 7026 Model M80 class computers have 6 GB of RAM, a 1.26 TB Shark storage array, and a gigabit Ethernet network connection.

As shown in FIG. 2, DB 400 is a centralized storage subsystem, which comprises numerous databases 430 housed in separate remote physical locations. Data is partitioned by its type and housed in distinct locations. Further, the DB 400 is capable of replicating itself to mirrored databases 430, located either on site or in separate sites.

In the preferred embodiment of the invention, a one to many search is utilized to scan the entire data set of enrolled biometric data resident on the DB 400 to determine the identity of

a user to allocate the appropriate account. The search and matching processing of the DB 400 may be implemented on servers containing multiple CPU's, each CPU working on a subset of the data. A massive parallel clustering scheme may be utilized to merge all processors within one server, or it's functional equivalent. Further, all operating data may be held in RAM at all times for maximum throughput.

Further, in the preferred embodiment, an efficient search and matching algorithm may be implemented with the DB 400 for an expeditious one to many search. An exemplary algorithm suitable for use in the preferred embodiment is the Veridicom Software Development Kit, Minutia Extraction Module and Fingerprint Verification Module, version linux-sdk-2.6.2.9-i386, available from Veridicom Incorporated, Santa Clara, CA. The Minutia Extraction Module scans and produces minutia based on features such as ridge endings, spacing, bifurcations, etc. Further, it extracts particularly significant minutia to perform a relative and distinct comparison between fingerprints; eliminating noisy minutia, borders, wrinkles, smudges, etc. The software produces templates of 1KB (uncompressed) or 300 bytes (compressed) for use with the Fingerprint Verification Module. The searching algorithm categorizes the stored fingerprint minutia into four categories: left loop, right loop, whirl, and neither. This categorization reduces the number of minutia to search and to match against hence, making the searching and matching process faster. The software scores these results, and provides statistics on matches relying on matching minutia based on distance, and neighborhood placement/orientation discrimination. This technique is capable of distinctly matching individuals based on discriminating minutia. Though the extraction module may extract many minutia, the matching set is very small based on the matching criteria mentioned above and allows the matching algorithm to be more efficient, since less minutia are being compared.

An alternate embodiment of a search and matching algorithm may be used as described in the United States Patent No. 5,802,525 to Isidore Rigoutsos, entitled "Two-Dimensional Affine-Invariant Hashing Defined Over Any Two-Dimensional Convex Domain and Producing Uniformly-Distributed Hash Keys", United States Patent No. 6,072,895 to Rudolf Maarten Bolle, et al., entitled "System and Method Using Minutiae Pruning for Fingerprint Image Processing", United States Patent No. 6,049,621 to Anil Jain, et al., entitled "Determining a Point Corresponding Between Two Points in Two Respective (Fingerprint) Images", United States Patent No.

6,041,133 to Andrea Califano, et al., entitled "Method and Apparatus for Fingerprint Matching Using Transformation Parameter Clustering Based on Local Feature Correspondence", United States Patent No. 6,005,963 to Rudolf Maarten Bolle, et al., entitled "System and Method for Determining if a Fingerprint Image Contains an Image Portion Representing a Partial Fingerprint Impression".

In another embodiment of the invention, the device may include a personal identifier that is assigned to each user to narrow the search parameters for matching biometric data. This personal identifier reduces the search from the entire set of data on the DB 400 to a manageable subset of data. The identifier is utilized to effectuate an enhanced rate of searching in the DB 400. The personal identifier may include but is not restricted to area codes, zip codes, or any other personal identifier representing the user's allocated group.

DB 400 Database server also includes local data memory, which is preferably implemented with the IBM DB2, version 6.1, relational database, which was designed to support both data and image storage within a single repository. This is a relational database management system ("RDBMS") for managing data operations between local data memory and application services. IBM DB2 is a commercially available software product of International Business Machines Corporation, New Orchard Road, Armonk, NY. The dynamic server of the preferred embodiment uses multiprocessing to efficiently process database 430 commands and other messages communicated through application services without delaying application service processing and communication with client subsystem 50 programs. Other embodiments of local data memory are possible as long as the embodiment is a highly available platform with sufficient storage and access times for the storage and retrieval of data. The database need not reside on a single physical platform; it may reside on several computing platforms comprising one logical unit, as in a database cluster. An application can access data from the client subsystem 50 and the server. Likewise, such an interface may be required when an application service is implemented in an object-oriented language such as C++ and local data memory is a relational database 430.

It is essential that the DB 400 is designed to store and house any and all types of information within user accounts including, but not limited to: biometric, financial, business,

personal, or academic; known henceforth as transactional data. User accounts are defined as storage allotted to each particular user within the DB 400. This system can receive, transmit, store, and process any type of transactional data, which may include but is not limited to: leases, deeds, passports, birth certificates, wills, trusts, driver's licenses, bank account information, credit information, commercial transaction information, educational information, citizenship information, photographs, pictures, digital sound files, digital graphic files, medical information, laboratory notes, grocery lists, personal dairies, to do lists, Christmas lists, digital movies, customer lists, trade secrets, computer source code, electronic mails, merchant inventory lists, cash flow information, expense information, consumer demographic information, sales information, payroll information, tax information, retirement information, investment information, benefits information, biometric information, incentive information, coupon information, governmental assistance program information, electronic cash, electronic signature information and voting information.

As known to persons of ordinary skill in the art, a relational database 430 consists of a collection of tables each of which have a unique name. See, e.g. Toerey, "Database Modeling & Design, Second Edition", chap. 2 and chap. 3, (Morgan Kaufmann Publishers, 1994). A database schema is the logical design of the database. Each table in a relational database has attributes. A row in a table represents a relationship among a set of values for the attributes in the table. Each table has one or more superkeys. A superkey is a set of one or more attributes, which uniquely identify a row in the table. A candidate key is a superkey for which no proper subset is also a superkey. A primary key is a candidate key selected by the database designer as the means to identify a row in a table.

As is well known to persons of ordinary skill in the art, the DataTreasuryTM Repository System 100 could use other database models available from other vendors including the entity relationship model as long as the selected database meets the storage access efficiency and synchronization requirements of the system. See, e.g., Toerey, "Database Modeling & Design, Second Edition", chap. 2 and chap. 3, (Morgan Kaufmann Publishers, 1994).

An exemplary DB 400 basic schema consists of the tables listed below. Since the names of the attributes are descriptive, they adequately define the attributes' contents. The primary keys in each table are identified with two asterisks (**).

I. CUSTOMER: This table describes the DataTreasury™ Repository System customer.

- A. **CUSTOMER.sub.-- ID
- B. COMPANY.sub.-- NAME
- C. CONTACT
- D. CONTACT.sub.-- TITLE
- E. ADDR1
- F. ADDR2
- G. CITY
- H. STATE.sub.-- CODE
- I. ZIP.sub.-- CODE
- J. COUNTRY.sub.-- CODE
- K. VOX.sub.-- PHONE
- L. FAX.sub.-- PHONE
- M. CREATE.sub.-- DATE

II. CUSTOMER.sub.-- MAIL.sub.-- TO: This table describes the mailing address of the DataTreasury™ Repository System customer.

- A. **MAIL.sub.-- TO.sub.-- NO
- B. **CUST.sub.-- ID
- C. CUSTOMER.sub.-- NAME
- D. CONTACT
- E. CONTACT.sub.-- TILE
- F. ADDR1
- G. ADDR2
- H. CITY
- I. STATE.sub.-- CODE
- J. ZIP.sub.-- CODE
- K. COUNTRY.sub.-- CODE
- L. VOX.sub.-- PHONE
- M. FAX.sub.-- PHONE
- N. CREATE.sub.-- DATE
- O. COMMENTS

In the preferred embodiment, through a communication network, the DB 400 is connected to the ORB 200 through a LAN using switched 1000BaseT/100BaseT Ethernet, and TCP/IP protocol though the invention is not so limited. As is known to persons of ordinary skill in the art, the 1000BaseT/100BaseT Ethernet is a networking link layer protocol. Further, the numbers 1000 and 100 refer to the communication link speed in megabits per second. In the

preferred embodiment the CISCO Catalyst 6000, model 6509, Network Switch or equivalent hardware supports the LAN connectivity between the devices connected to it. However, DB 400 could also connect to ORB using a WAN connection shown in FIG. 8.

Fig. 6 displays the block diagram of the DataTreasury™ Encryption Subsystem (ES) 500. The ES 500 ensures a secure transaction and communication between the DataTreasury™ Application Server (AS) 300 and their client subsystems 50. Furthermore, the ES 500 ensures that all data stored is encrypted and secured against any attempts to gain unauthorized access. Encryption which protects against unauthorized access for use in the present invention is described in United States Patent No. 5,910,988, United States Patent No. 6,032,137, and United States Patent Application 09/454,492 to Ballard, entitled "Remote Image Capture with Centralized Processing and Storage", which patent is incorporated herein by this reference. The ES 500 is further capable of detecting potential tampering of documents in transit. Lastly, the ES 500 verifies the identity of the client subsystem 50 initiating the transaction. The ES 500 is created as an encryption object initiated from the AS 300.

One embodiment of the cryptography scheme in the ES 500, is implemented with a symmetric cryptography scheme. Symmetric cryptography entails the use of a single secret key for both encryption and decryption of the transmission. The client subsystem 50 and the AS 300 require the possession of the key issued to the client subsystem 50 in order to decipher transmissions. The AS 300 issues unique keys to each of their client subsystems 50.

Another embodiment of the cryptography scheme in the ES 500, is implemented with an asymmetric cryptography scheme. An asymmetric scheme utilizes a two key pair, which consists of a public key 520 and a private key 580. A public key 520 is one that is freely distributed, whereas a private key 580 is treated in a surreptitious fashion. A document that is encrypted with public key 520 may only be decrypted with the corresponding private key 580, and visa versa.

Furthermore, the integrity of the communications within the ES 500 may be ensured with the use of a digital signature. A digital signature is used to link the owner of the public key to the document; it is also capable of detecting alterations to the transmission in transit. The transmission is subjected to an encryption process, known to a person skilled in the art as

hashing, and a message digest is created. The process of creating the message digest is known as the digesting process. A message digest is a unique value of fixed length dependent on the input into the digesting process transmission. Both parties need to be aware that the digesting process is utilized.

Once the user formulates the desired transmission, it is then subjected to the digesting process. Then the client subsystem 50 utilizes his public key to encrypt the message digest and the transmission, which results in a digital signature. The digital signature can be combined with the transmission, or exist as a separate entity. The AS 300 receives the transmission along with the digital signature. The digital signature is decrypted utilizing the corresponding private key to obtain a decrypted message digest. The transmission is then subjected to the digest process to obtain a message digest. Lastly, the ES 500 compares the signature message digest with the transmission message digest, if these values are equal, then the client subsystem 50 is authenticated.

Another method that may be used to ensure data transmission authenticity is the use of digital certificates 550. These digital certificates 550 certify the identity of the holder of the public key 520. The AS 300 may act as a certification authority 560. The certification authority 560 issues the digital certificates 550 to client subsystems 50. The digital certificates 550 verify that the owner of the public key 520 is also the certificate holder.

The client subsystem 50 obtains the digital certificate 550 and presents it to the application with some form of identity verification, specifically, but not exclusively biometric information, personal information, financial information. The application verifies the certificate with the certificate authority 560, and the AS 300. The digital certificate 550 which is sent to the client subsystem 510 may contain one or more of the following: the certification authority's 560 digital signature, the public key 520 of the client subsystem 510, the name of the user, the name of the certification authority 560, and the expiration date of the certificate.

Data is stored in the DB 400 in an encrypted form. After retrieval from the database the records must be decrypted before any useful operation can be performed on them. For decryption, a cryptographic key is required. The key is obtained as a result of, or in conjunction

with, the authentication process using a biometric. In this way, it is possible to secure records from access from all but the authentic owner of the information.

The DataTreasury™ Repository System 100 is not so limited to the encryption and the authentication schemes. As known to persons of ordinary skill in the art, the DataTreasury™ Repository System may utilize any scheme that ensures the highest degree of security, encryption and authentication may also be implemented. See, e.g., Pleege, "Security in Computing", Second Edition, chap. 2 to chap. 9, (Prentice Hall, 1996).

Fig. 7 displays a block diagram of the process for processing biometrics using the DataTreasury™ Biometric Subsystem (DTBS) 600. The DTBS 600 processes all biometric information in the DataTreasury™ Repository System. The DTBS 600 may make use of layered biometrics for added security. A layered biometric consists of multiple types of biometrics or multiples of the same type biometric. The biometric information may be from a fingerprint, digital voiceprint, retinal scan, DNA or some other form of biometric. The multiple biometric sources are individually processed, and a composite of the resulting elements are used for verification. The DTBS 600 extracts minutia from the fingerprint and stores them in the DB 400. The DTBS 600 further authenticates the user identity with their personal biometric. Devices for capturing biometrics which are subsequently utilized to verify the identity of a person by comparing the biometric data captured remotely with the biometric data stored for use in the present invention are described in United States Patent No. 5,910,988, United States Patent No. 6,032,137, and United States Patent Application 09/454,492 to Ballard, entitled "Remote Image Capture with Centralized Processing and Storage", which is incorporated herein by reference.

In the fingerprint biometric subsystem, a capacitive apparatus may be utilized to capture a biometric signature, preferably in the form of a raw image 605 of the fingerprint. This biometric device is connected to the client subsystem 50. The fingerprint may then be saved in an image format. It may also be compressed with a loss-less compression algorithm, and/or converted to a more efficient image format. An apparatus stated in the U.S. Patent entitled "Capacitive Fingerprint Sensor with Adjustable Gain," 6,049,620, may be utilized.

The compressed and then encrypted image is then transferred to the DataTreasury™ Repository System. In the preferred embodiment, once the image has been received, the AS 300

begins preprocessing 610 the image. Preprocessing 610 performs basic image enhancement transformations on the image, such as the adjustment of: contrast, brightness, and scale, and additionally removes extraneous noise from the image to produce an enhanced image of the fingerprint. Preprocessing 610 can correct for differences in images due to acquisition using different sensors, as well as other variables affecting image acquisition. It is also possible to create profiles for specific devices or conditions, and apply them conditionally during preprocessing 610.

After preprocessing 610 is complete, the image is subjected to a binarization process 615. The binarization process 615 transforms the image into pixels of values either pure black or white.

Skeleton processing 617 follows binarization. The skeleton image is formed by reducing the lines representing finger ridges in the binary image to a width of 1 pixel wide. This is done to maintain the original topography and connectivity of the ridges. Skeleton postprocessing is then conducted to enhance the skeleton image by interpolating breaks in the skeleton images caused by finger pores, scars, wrinkles, and other surface imperfections in the finger. See, e.g., Jain, Halici, Hayashi, Lee, and Tsutsui, "Intelligent Biometric Techniques in Fingerprint and Face Recognition", chap. 2 and chap. 3, (CRC Press, 1999).

The image is then classified in step 630 into distinct categories to decrease retrieval time. These categories may include but are not limited to: whorls, loops, and arches. These categories are utilized to form an index of the client subsystem's 50 identity corresponding to minutia within DB 400. For instance, a process in the U.S. Patent entitled "Neural Network System for Classifying Fingerprints," U.S. Patent Number 5,825,907 may be utilized to classify fingerprints.

The minutia points are extracted in step 650. An algorithm is utilized to obtain minutia points. If the extracted minutia points cannot be read, then in step 670 DTBS 600 utilizes a different biometric and then in step 695 repeats the comparison of biometrics. However if DTBS 600 can read the biometrics, then the extracted minutia points are compared in step 675 with the point of reference minutia points resident in DB 400. The point of reference, enrollment minutia are obtained and subsequently stored in the DB 400 during the user's registration process. If the minutia points match in step 690, a positive verification is made. However, if there is no match,

then another biometric input 670 is requested, and verification fails. The other biometric may be from another type of biometric input 670, like a voiceprint or retinal print. Furthermore, it may be from another source input of the same type of biometrics. This other biometric 670 is reintroduced into the verification process 695.

FIG. 8 shows a block diagram of communication network 800 connecting client subsystems 50, hosts 70 ORB 200, and DB 400. ORB 200 may connect to other ORB 200 systems via a first local area network or LAN connection 810 which contains a network switch 812. Client subsystems 50 and hosts 70 may be connected to each other via the internet or via an ethernet connection forming an intranet. Both client subsystems 50 and hosts 70 connect to API 80 or SOS 90 first and then to ORB 200 via a wide area network or WAN connection 820. WAN connection 820 comprises an ethernet network 822 connected to client subsystems 50 or hosts 70 and another ethernet network 823 connected to network switch 812. Ethernet 822 associated with client subsystems 50 connects to a WAN router 824 while ethernet 823 associated with network switch 812 connects to WAN router 825. WAN routers 824 and 825 connect to API Gateway 80 or SOS 90 via network lines 823. API Gateway 80 or SOS 90 connects to network switch 812 which connects to ORB servers 200.

ORB 200 also connects to DB 400 via a second LAN 840. In addition DB 400 may exist as one or more servers connected to each other via a second LAN 860 containing a network switch 862. Second LAN 840 comprises an ethernet network, for connecting to network switch 812 for ORB 200 and for connecting to network switch 862 for DB 400. Network switch 862 connects to data storage subsystems DB 400.

This invention is not so limited by the method of extracting and analyzing minutia.

For example, FIG. 9 is a flowchart depicting the general process for the central management, security, storage, biometric authentication, verification and user or initiator initiated data transactions.

Thus this process includes a first step 910 which includes capturing transactional data including an image of the biometric data, and any and all types of additional data. Next, in step 920 at least one remote location encrypts and sends this transactional data or information. In

step 930, the authenticity and identity of the user is verified so that the user can access an appropriate account. In step 940, the transactional data is encrypted and decrypted upon transmission and storage and presentation to the user. In step 950 the capturing and sending of data is managed. Next, in step 960, this data is collected at a remote centralized location. In step 970, the remote centralized location manages the collecting, processing, sending and storing of this transactional data. Finally, in step 980 the encrypted transactional data and subsystem identification information is transmitted between the remote location the centralized location and other entities.

Step 910 which comprises the step of capturing transactional data may include the steps of capturing biometric data and any and all additional data; successively transforming the captured biometric data to a biometric signature, creating an encrypted compressed file identifying a location and time of the biometric data capturing; storing the tagged, encrypted compressed biometric signature file; and initiating a transaction upon the capture of a biometric.

Step 920 which includes the step of encrypting the data includes the steps of creating encryption keys to encrypt the data; and encrypting and decrypting the transactional data with encryption and decryption keys.

Steps 910 and 920 can occur at a plurality of remote locations while step 960 which includes collecting processing sending and storing the encrypted transactional data at a remote centralized location can occur at a plurality of independent locations. Step 960 may also include the steps of transmitting from remote locations transactional data with servers at a centralized location; storing specific types of encrypted transactional data at distinct independent remote locations in a memory hierarchy, wherein the storing of this data maintains recently accessed encrypted transactional data in a primary memory and other encrypted transactional data in a secondary memory; dynamically assigning the servers at the central location to receive portions of the transactional data for balancing

Fig. 10 is a flowchart depicting the operation of one embodiment of the present invention.

In step 1010, a registered user who desires a service from the DataTreasury™ Repository System initiates a transaction. The user begins the transaction by inputting a biometric. Client subsystem 50 transactions are associated with unique stubs.

In step 1020, a client subsystem 50 stub resides at the terminal; and the stub forwards the transaction via frame relay. All transmissions sent to the ORB 200 are encrypted.

In step 1030, the crypto object verifies that the stub is a valid DataTreasury™ Repository issuer. The crypto subsystem verifies secure communication between the stub and skeleton using but not limited to socket level cryptography. Lastly, the crypto object decrypts the messages.

In step 1040, the skeletons specify all objects to be created to accomplish the desired task.

In step 1050, the business application objects associated with the identified skeletons are invoked by the ORB 200. The AS 300 instantiates the business objects, to correspond with the skeletons.

In step 1060, the business application object instantiates a biometric verification object to ensure the identification of the user with the corresponding level of confidence.

In step 1070, the raw fingerprint is grafted on a vector grid to extract invariant characteristics, such as minutia points. The minutia extraction is accomplished through an algorithm.

In step 1080, the ORB 200 initiates a query of the DB 400, amongst the enrolled user biometrics store, for minutia matches. This can be but not limited to a one-to-one search when there exists no personal identifier. When there is such a personal identifier available, the parameters of the one-to-many search are dramatically reduced. Lastly, the minutia points are matched.

In step 1085, the AS 300 business objects perform the client subsystem 50 requested operation on the user account corresponding to the user's biometric.

In step 1090, the encrypted response/results are returned to the client subsystem 50.

FIG. 11 is a second embodiment of the flowchart shown in FIG. 9. In this case, many of the steps shown in FIG. 9 are shown. For example, in step 910 transactional data is captured, while in step 920, this data is encrypted and sent. However, instead of verifying the authenticity of the user in step 930, the system verifies the identity of the user in step 931. This step involves a one to many search wherein the system searches for the user's identity which has been previously stored in DB 400. Once this identity has been matched, in step 933 the system creates a pseudo identifier which identifies the user via a limited information tag such as a set of demographic information. In step 935, this pseudo identifier is stored in a pseudo identifier database in DB 400. Next, in step 937, the system sets a security filter so that this pseudo identifier and cannot be used to determine the true identity of the user.

Once the user's pseudo identification has been established, the system proceeds through steps 940-980 as in FIG. 9. This type of process shown in FIG. 11 can be used especially for voting or health care where the identity of the user must remain secret. If this process is used for voting then step 910, which is the step of capturing transactional data, includes capturing voting information such as the votes cast by each user. If this process is used for health care, then step 910 involves capturing the health history of the user, the health care insurance information of the user, or any health related tests for the user such as blood tests or urine tests.

While the above invention has been described with reference to certain preferred embodiments, the scope of the present invention is not limited to these embodiments. One skilled in the art may find variations of these preferred embodiments which, nevertheless, fall within the spirit of the present invention, whose scope is defined by the claims set forth below.

WHAT IS CLAIMED IS:

1. A system to provide a centralized, secured and authenticated storage of information comprising:

a) at least one client subsystem to receive and send transactional data comprising:

5 i) at least one biometric processing client subsystem for capturing biometric data; and

ii) at least one data capturing device to capture any and all types of additional data;

10 b) at least one remote data management subsystem for managing the processing, sending receiving, and storing of the transactional data;

c) at least one remote data storage subsystem to store any and all transactional data;

15 d) at least one data processing subsystem for processing all transactional data, with the client subsystem providing encrypted subsystem identification information and encrypted transactional data to the data processing subsystem;

e) at least one biometric subsystem to verify the user's identity, and at least one encryption subsystem for ensuring the security of the transactional data; and

20 f) at least one communication network for secure transmission of transactional data within and between said at least one client subsystem, and said at least one data management subsystem.

2. The system, as in claim 1, wherein said at least one client subsystem further comprise at least one biometric device for capturing biometric data.

3. The system, as in claim 2, wherein said at least one client subsystem successively transforms the captured biometric data to an encrypted image format, a compressed image file, data transmission identifying a location and time of the transactional data capture,

further comprising at least one transaction stub for interfacing to the data management subsystem.

4. The system, as in claim 1, wherein said at least one client subsystem further comprise at least one input device for capturing any and all types of additional data.

5. The system, as in claim 4, wherein said at least one client subsystem successively encrypts the transactional data, which further comprises at least one transaction stub for interfacing a transaction management subsystem.

6. The system, as in claim 2, wherein said at least one input of biometric data facilitates a client transaction.

7. The system as in claim 1, wherein said at least one encryption subsystem creates, utilizes, and stores keys to encrypt and decrypt transactional data.

8. The system, as in claim 6, wherein said at least one client subsystem further comprises at least one printer for printing the transactional data initiated by said at least one biometric interface.

9. The system, as in claim 1, wherein said data management subsystem comprises:
at least one server providing for resources for processing, and
managing the storage of transactional data from said at least one remote client subsystem;
at least one report generator for generating reports from the
5 transactional data;
a transaction processing architecture for dynamically administrating a
series of intelligent data management services among said at least one server; and
a memory hierarchy.

10. The system, as in claim 9, wherein said at least one server contains an object oriented programming language.

11. The system, as in claim 9, wherein said processing of transactional data by said data processing subsystem occurs after said transactional data is decrypted by said encryption subsystem.

12. The system, as in claim 9, wherein said transactional data is re-encrypted by said encryption subsystem after said data processing and said data is then stored in said data storage subsystem.

13. The system, as in claim 9, wherein said at least one transaction processing architecture contains a CORBA object request broker (ORB) architecture, that apportions and balances transactional resources among at least one server.

14. The system, as in claim 13, wherein said at least one ORB architecture utilizes an interface definition language (IDL) and an IDL compiler to create an interface between application components.

15. The system, as in claim 14, wherein said at least one IDL compiler generates a series of stubs and skeletons to facilitate an interface.

16. The system, as in claim 9, wherein said at least one server also receives encrypted transactional data, said data storage subsystem stores the encrypted transactional data, and said at least one server verifies the biometric data.

17. The system, as in claim 16, wherein said at least one biometric subsystem reduces the biometric data to a series of invariant characteristics through the use of an algorithm.

18. The system, as in claim 17, wherein said at least one server utilizes a biometric search algorithm to facilitate a one to many search to identify a corresponding data storage subsystem resident enrolled biometric to verify the user.

19. The system, as in claim 18, wherein said at least one server identifies an appropriate user account corresponding a verified user biometric.

20. The system, as in claim 17, wherein said at least one server has a personal identifier to reduce the parameters of the one to many search to identify a corresponding data storage subsystem with a corresponding enrolled biometric to verify the user.

21. The system, as in claim 20, wherein said at least one server identifies the appropriate user account corresponding to a verified user biometric.

22. The system, as in claim 9, wherein said memory hierarchy comprises at least one primary memory for storage of recently accessed encrypted transactional data and at least one secondary memory for storage of other encrypted transactional data.

23. The system, as in claim 22, wherein said at least one secondary memory comprises at least one magnetic media.

24. The system, as in claim 22, wherein said at least one secondary memory comprises a plurality of data stores housed in separate distinct remote physical locations.

25. The system, as in claim 24, wherein said specific data stores, house unique types of data.

26. The system, as in claim 1, wherein said at least one communication network comprises:

at least one first local area network for transmitting data within a corresponding one of said at least one remote client subsystem;

5 at least one second local area network for transmitting data within a corresponding one of said at least one data management subsystem; and

at least one wide area network for transmitting data between said at least one remote client subsystems and said at least one data management subsystem.

27. The system, as in claim 26, wherein said at least one communication network further comprises:

at least one Ethernet for connecting said at least one first local area network of said at least one client subsystems to a corresponding one of said at least one
5 second local area network of said at least one data management subsystem through said at least one wide area network; and

at least one frame relay for connecting said at least one second local area network of said at least one data management subsystem to a corresponding one or more of said at least one first local area network of said at least one client subsystems through
10 said at least one wide area network.

28. The system, as in claim 26, wherein said at least one communication network comprises a wireless network between said at least one remote client subsystems and said at least one data management subsystem.

29. The system, as in claim 28, wherein said at least one wireless network may be implemented utilizing various technologies selected from the group consisting of:

a cellular communication network;

a personal communications services network;

5 a k-band technology;

- an infrared technology;
a local multipoint distribution system;
a satellite system;
a microwave technology;
10 a radio frequency technology;
a code division multiple access technology;
a time division multiple access technology;
a global system for mobile communication system;
a bluetooth technology;
15 a plurality of wireless application protocols; and
a wide area point to point network technology.

30. The system, as in claim 1, further comprising at least one data collecting subsystem for collecting and sending the transactional data comprising a further data management subsystem for managing the collecting and sending of the transactional data.

31. The system, as in claim 30, wherein said further data management subsystem of said at least one data collecting subsystem comprises:

- at least one server for receiving said at least one remote client subsystems for transactional data;
5 a database for storing the transactional data in a useful form;
at least one server for managing the collecting of the transactional data;
a transaction processing architecture for dynamically assigning one of said at least one server to receive portions of the transactional data for balancing the transactional data among said at least one server; and
10 a memory hierarchy.

32. The system as in claim 9, wherein said at least one server has an object oriented programming language.

33. The system as in claim 9, wherein said at least one transaction processing architecture has a CORBA ORB architecture, that apportions and balances transactional resources.

34. The system as in claim 33, wherein said at least one server has an interface definition to create an interface between application components.

35. The system as in claim 34, wherein said at least one IDL compiler generates stubs and skeletons to create an interface.

36. The system, as in claim 31, wherein said memory hierarchy comprises at least one primary memory for collecting transactional data and at least one secondary memory for backup storage of the encrypted transactional data.

37. The system, as in claim 36, wherein said at least one secondary memory comprises at least one tape library.

38. The system as in claimed 37, wherein said at least one secondary memory comprises numerous data stores housed in separate distinct physical locations.

39. The system as in claim 38, wherein said specific data stores house unique types of data.

40. The system, as in claim 30, wherein said at least one communication network comprises:

at least one first local area network for transmitting encrypted transactional data within a corresponding one of said at least one remote client subsystems;

at least one second local area network for transmitting encrypted transactional data within a corresponding one of said at least one data collecting subsystem;

at least one third local area network for transmitting encrypted transactional data within a corresponding one of said at least one data processing subsystem; and

10 at least one wide area network for transmitting encrypted transactional data between said at least one remote client subsystems, said at least one data collecting subsystem and said at least one data processing subsystem.

41. The system, as in claim 40, wherein said at least one communication network further comprises:

at least one first Ethernet network for connecting said at least one first local area network of said at least one client subsystems to a corresponding one of said at
5 least one second local area network through said at least one wide area network;

at least one frame relay for connecting said at least one second local area network of said at least one data collecting subsystem to a corresponding some of said at least one first local area network of said at least one client subsystems through said at least one wide area network;

10 at least one first wide area network router for connecting a corresponding one of said at least one second local area network of said at least one data collecting subsystem to said at least one wide area network; and

at least one second wide area network router for connecting a corresponding one of said at least one third local area network of said at least one data
15 processing subsystem to said at least one wide area network.

42. The system, as in claim 41, wherein said at least one first wide area network and said at least one second wide area network comprises a carrier cloud, said carrier cloud using a frame relay method for transmitting the transactional data.

43. The system, as in claim 42, wherein said at least one second local area network and said at least one third local area network further comprises a corresponding one of at

least one network switch for routing transactional data within said at least one second local area network and said at least one third local area network.

44. The system, as in claim 40, wherein said at least one wireless network may be implemented utilizing various technologies which further comprise:

- a cellular communication network;
- a personal communications services network;
- 5 a k-band technology;
- an infrared technology;
- a local multipoint distribution system;
- a satellite system;
- a microwave technology;
- 10 a radio frequency technology;
- a code-division multiple access technology;
- a time division multiple access technology;
- a global system for mobile communication system;
- a bluetooth technology;
- 15 a plurality of wireless application protocols; and
- a wide area point to point network technology.

45. A method for central management, security, storage, biometric authentication, verification, and initiator initiates data transactions comprising the steps of:

capturing transactional data including an image of the biometric data, further any and all types of additional data, at at least one remote locations encrypting, and
5 sending encrypted transactional data;

verifying the authenticity of the user using a one to one search for access to an appropriate account;

encrypting transactional data upon transmissions and storage, further decrypting data upon processing and presentation to the authorized user;

10 managing the capturing and sending of the transactional data;

collecting, processing, sending and storing the encrypted transactional data at a remote centralized location;

managing the collecting, processing, sending and storing of the transactional data; and

15 transmitting the encrypted transactional data and a subsystem identification information within and between the remote location(s), the centralized location(s), and other entities.

46. The method as in claim 45, wherein said capturing the transactional data which includes biometric data step comprises:

capturing biometric data;

5 successively transforming the captured biometric data to a biometric signature, an encrypted, compressed file identifying a location and time of the biometric data capturing;

storing the tagged, encrypted, compressed biometric signature file; and initiating a transaction upon the capture of a biometric.

47. The method as in claim 46, wherein said capturing step of the transactional data which includes any and all additional types of data, comprises:

capturing any and all additional types of data;

5 successively encrypting the data, identifying a location and time of the data capturing; and

storing the tagged, encrypted, compressed biometric signature file.

48. The method, as in claim 45, wherein said encrypting step comprises the steps of:

creating encryption keys to encrypt data; and

encrypting and decrypting transactional data with the encryption and decryption keys.

49. The method, as in claim 45, wherein:

said biometric capturing and sending step occurs at a plurality of remote locations; and

5 said collecting, processing, sending and storing step occurs at a plurality of independent locations.

50. The method, as in claim 49, wherein said collecting, processing, sending and storing step comprises the steps of:

remote locations transmitting transactional data with servers at the central locations;

5 storing specific types of encrypted transactional data at distinct independent remote locations in a memory hierarchy, said storing maintains recently accessed encrypted transactional data in a primary memory and other encrypted transactional data in a secondary memory;

10 dynamically assigning the servers at the central location to receive portions of the transactional data for balancing the transactional data among the servers; and generating reports from the transactional data and providing data to software applications.

51. The method, as in claim 50, wherein said storing the encrypted transactional data step comprises the step of partitioning the stored transactional data into tables.

52. The method, as in claim 51, wherein said searching the memory for matching biometric data step comprises:

transmitting captured biometric data from remote locations to centralized servers at the remote independent locations;

5 reducing the captured biometric data to the invariant characteristics with an algorithm; and

conducting a search of the enrolled user biometric data resident in memory stores.

53. The method, as in claim 52, wherein said searching of the enrolled user biometric comprises:

utilizing a one to many search to scan the complete data store of the enrolled user biometrics through the use of a one to many biometric search algorithm for the matching biometrics;

comparing the captured biometric data to stored enrolled biometric data respectively for identification verification; and

allowing verified and authenticated user access to the authorized user account.

54. The method, as in claim 52, wherein said searching of the enrolled user biometric comprises:

utilizing a personal identifier for each user;

reducing the search to a smallest subset possible with the personal identifier;

conducting a one-to-many search for matching biometric data;

comparing the captured biometric data to stored enrolled biometric data respectively for identification verification; and

allowing verified and authenticated user access to the authorized user account.

55. The method, as in claim 52, wherein said transmitting the encrypted transactional data step comprises the steps of:

transmitting data within the remote locations;

transmitting data from each remote location to a corresponding central

location; and

transmitting data within the central locations.

56. The method, as in claim 55, wherein said transmitting data from each remote location to a corresponding central location step comprises the steps of:

connecting each remote location to a corresponding central location;

and

connecting each central location to corresponding remote locations.

57. The method, as in claim 49, further comprising the steps of:

collecting and sending the encrypted transactional data at intermediate locations;

managing the collecting and sending of the encrypted transactional data; and

transmitting the encrypted transactional data within the intermediate location and between the intermediate locations and the remote locations and the central locations.

58. The method, as in claim 57, wherein said managing the collecting and sending step comprises the steps of:

polling the remote locations for transactional data with servers in the intermediate locations;

storing the encrypted transactional data in the intermediate locations, said storing step maintaining the encrypted transactional data in a primary memory of a memory hierarchy and performing backup storage of the encrypted transactional data into a secondary memory of the memory hierarchy; and

dynamically assigning the servers to receive portions of the encrypted transactional data for balancing the encrypted transactional data among the servers.

59. The method, as in claim 57, wherein said step of transmitting the encrypted transactional data comprises the steps of:

transmitting the encrypted transactional data within the remote locations;

5 transmitting the encrypted transactional data from each remote location to a corresponding intermediate location;

transmitting the encrypted transactional data within the intermediate locations;

10 transmitting the encrypted transactional data from each intermediate location to corresponding central locations; and

transmitting the encrypted transactional data within the central locations.

60. The method, as in claim 59, wherein said transmitting data from each remote location to corresponding intermediate locations step comprises the steps of:

connecting each remote location to a corresponding intermediate location; and

5 connecting the intermediate locations to corresponding remote locations.

61. The method, as in claim 59, wherein said transmitting data from each intermediate location to corresponding central locations comprises the steps of:

connecting each intermediate location to an external communication network; and

5 connecting the corresponding central locations to the communication network.

62. The method as in claim 49, wherein said transmitting data from each intermediate location to corresponding central locations comprises the steps of:

connecting each intermediate location to an external communication network; and

5 connecting the corresponding central locations to the communication network.

63. A system to facilitate financial commercial transactions between a buyer and a seller through the stored information, wherein each party may select from financial accounts on file to facilitate requests for credits and/or debits through financial institutions comprising:

5 at least one client subsystem to facilitate user requested transactions, wherein biometric data is captured through a biometric device and further at least one input device to capture any and all transactional data;

at least one transaction processing architectural system to manage processing, sending, receiving and storage of transactional data;

10 at least one data processor to facilitate the processing, encrypting, Personal Identification Number (PIN)-less and Personal Identification Card (PIC)-less searching and biometric matching of the transactional data;

at least one database to store transactional data; and

at least one communication network to facilitate user access to the system
15 through the client subsystems, and to interconnect the client subsystems with the data
processing subsystem, the storage subsystems, and other external entities.

64. A method to facilitate financial commercial transactions between a buyer and a
seller through the stored information, wherein each party may select from financial accounts
on file to facilitate requests for credits and/or debits through financial institutions
comprising:

- 5 verifying users through a PIN-less and PIC-less, one to many search of an
enrollment storage subsystem, to allocate the appropriate user account to be accessed;
- managing data processing, and storage through the use of an intelligent data
management subsystem;
- populating requested transaction fields for the transaction;
- 10 requesting a credit and/or debit from financial institutions;
- transmitting and receiving transactional data from external entities; and
- storing any and all transactional data within the data storage subsystem.

65. A system to facilitate transactions between biometrically verified users through
stored information, wherein information required of the transaction may be populated from
the storage subsystem comprising:

- at least one client subsystem to facilitate user requested transactions, wherein
- 5 biometric data is captured through a biometric device and further at least one input device to
capture any and all transactional data;
- at least one transaction processing architectural system to manage processing,
sending, receiving and storage of transactional data;
- at least one data processor to facilitate the processing, encrypting, PIN-less and
- 10 PIC-less searching and biometric matching of the transactional data;
- at least one database to store transactional data; and
- at least one communication network to facilitate user access to the system
through the client subsystems, and to interconnect the client subsystems with the data
processing subsystem, the storage subsystems, and other external entities.

66. A method to facilitate transactions between biometrically verified users through stored information, wherein information required of the transaction may be populated from the storage subsystem comprising:

- 5 verifying the users through a PIN-less and PIC-less, one to many search of an enrollment storage subsystem to allocate the appropriate authorized user account to access;
- managing data processing, and storage through the use of an intelligent data management subsystem;
- populating requested transaction fields for the transaction;
- requesting a credit and/or debit from financial institutions;
- 10 transmitting and receiving transactional data from external entities; and
- storing any and all transactional data within the data storage subsystem.

67. A method for central management, security, storage, biometric authentication, verification, and initiator initiates data transactions comprising the steps of:

- 5 capturing transactional data including an image of the biometric data, further any and all types of additional data, at at least one remote locations encrypting, and sending encrypted transactional data;
- verifying the identity of a user using a one to many search for access to an appropriate account;
- encrypting transactional data upon transmissions and storage, further decrypting data upon processing and presentation to the authorized user;
- 10 managing the capturing and sending of the transactional data;
- collecting, processing, sending and storing the encrypted transactional data at a remote centralized location;
- managing the collecting, processing, sending and storing of the transactional data; and
- 15 transmitting the encrypted transactional data and subsystem identification information within and between the remote location(s), the centralized location(s), and other entities.

68. The method as in claim 67, wherein said step of capturing transactional data includes capturing voting data from said user.

69. The method as in claim 67, wherein said step of capturing transactional data includes capturing health care data from said user, including said user's health related history and said user's health insurance information.

70. The method as in claim 67, further comprising the step of creating a pseudo identifier for said user.

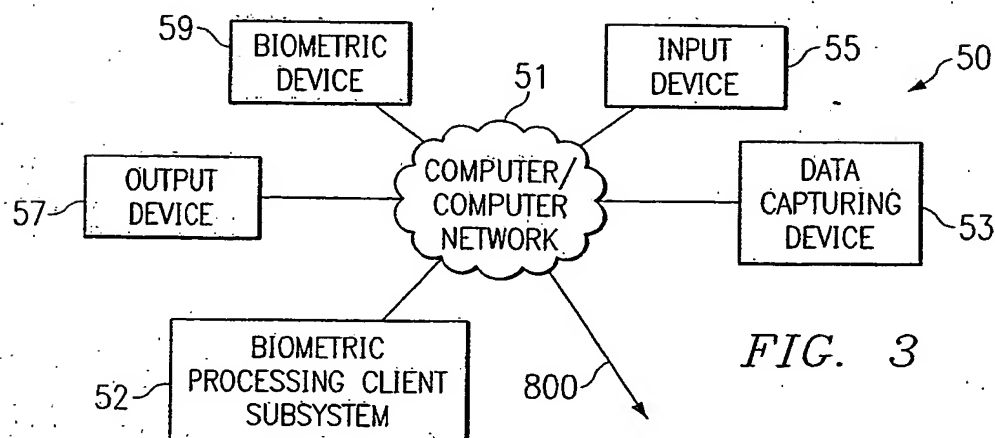
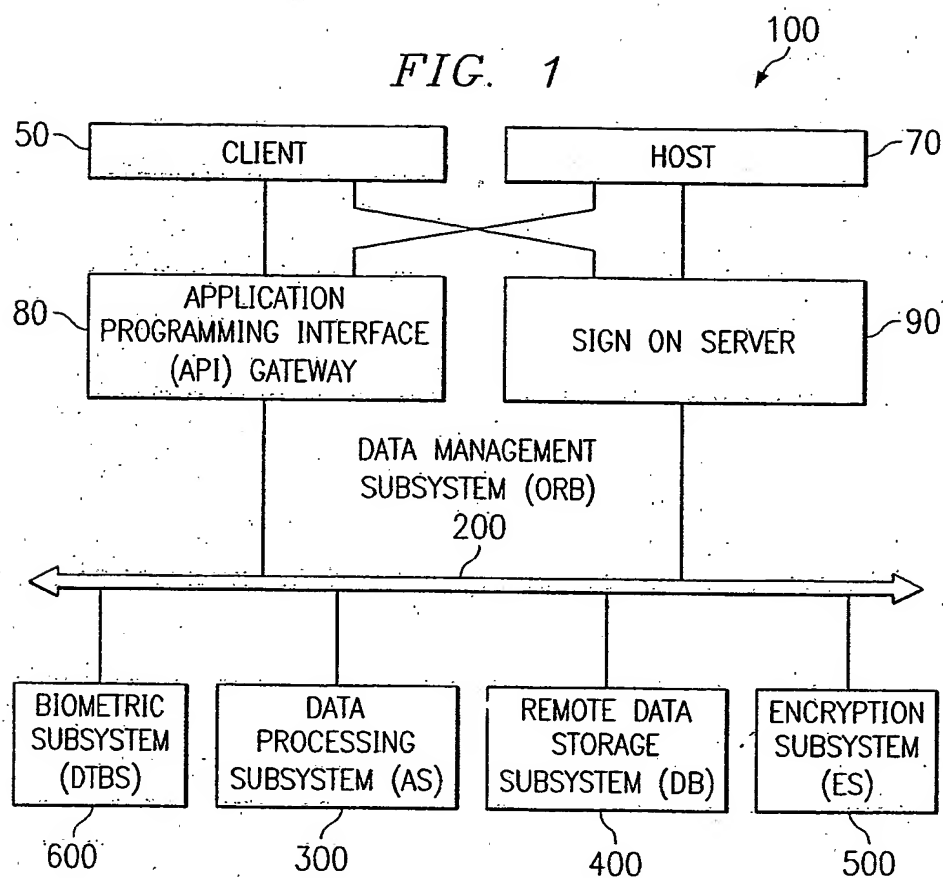
71. The method as in claim 70 wherein said pseudo identifier is a demographic tag that can be set to reveal any and all information relating to the user.

72. The method as in claim 70, wherein said step of creating a pseudo identifier occurs after said step of identifying said user.

73. The method as in claim 70 further comprising the step of storing said pseudo identifier in a pseudo identifier database.

74. The method as in claim 73, further comprising the step of setting a security filter so that said pseudo identifier and said pseudo identifier database do not reveal said user's original identity.

1/7



2/7

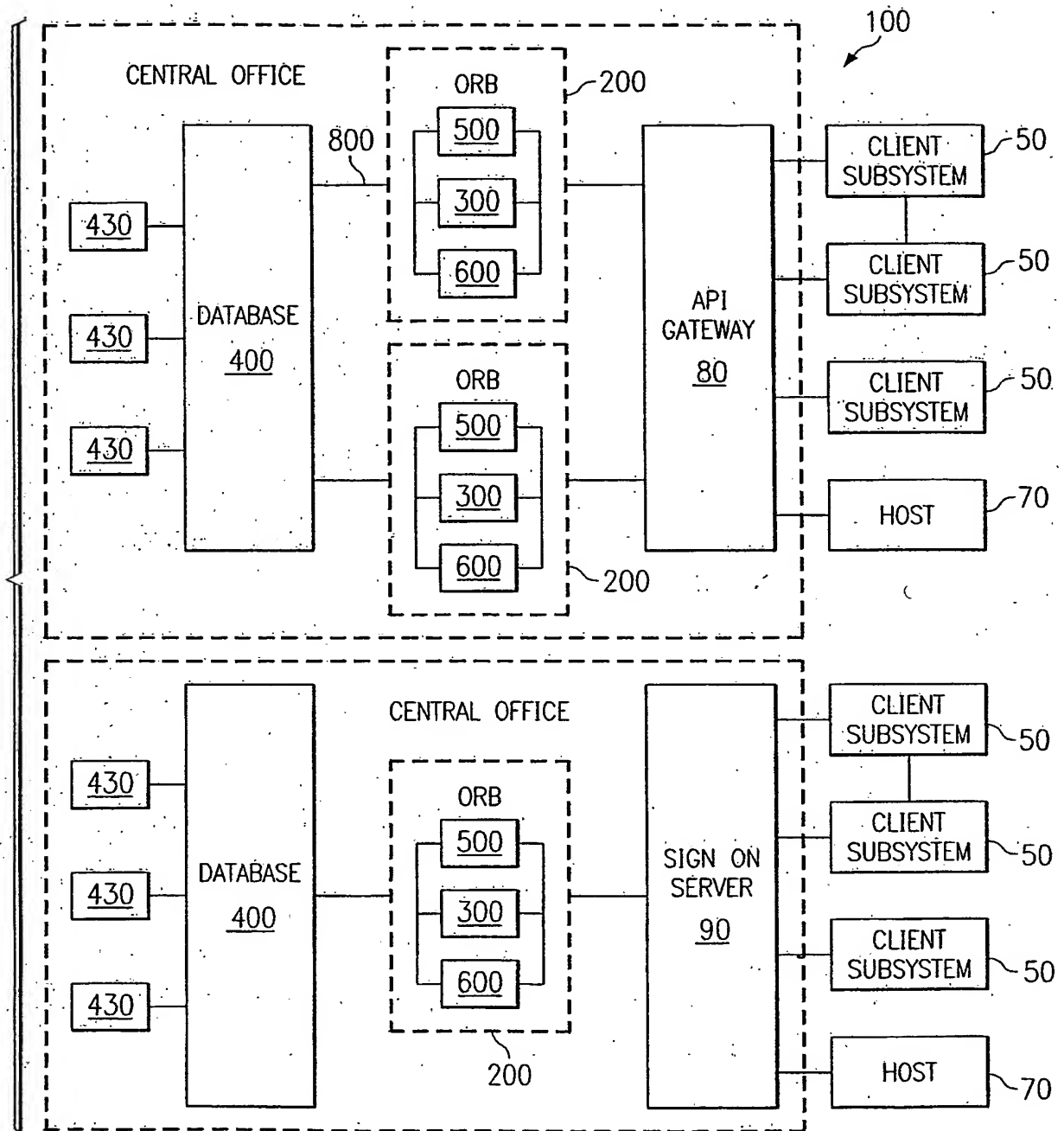
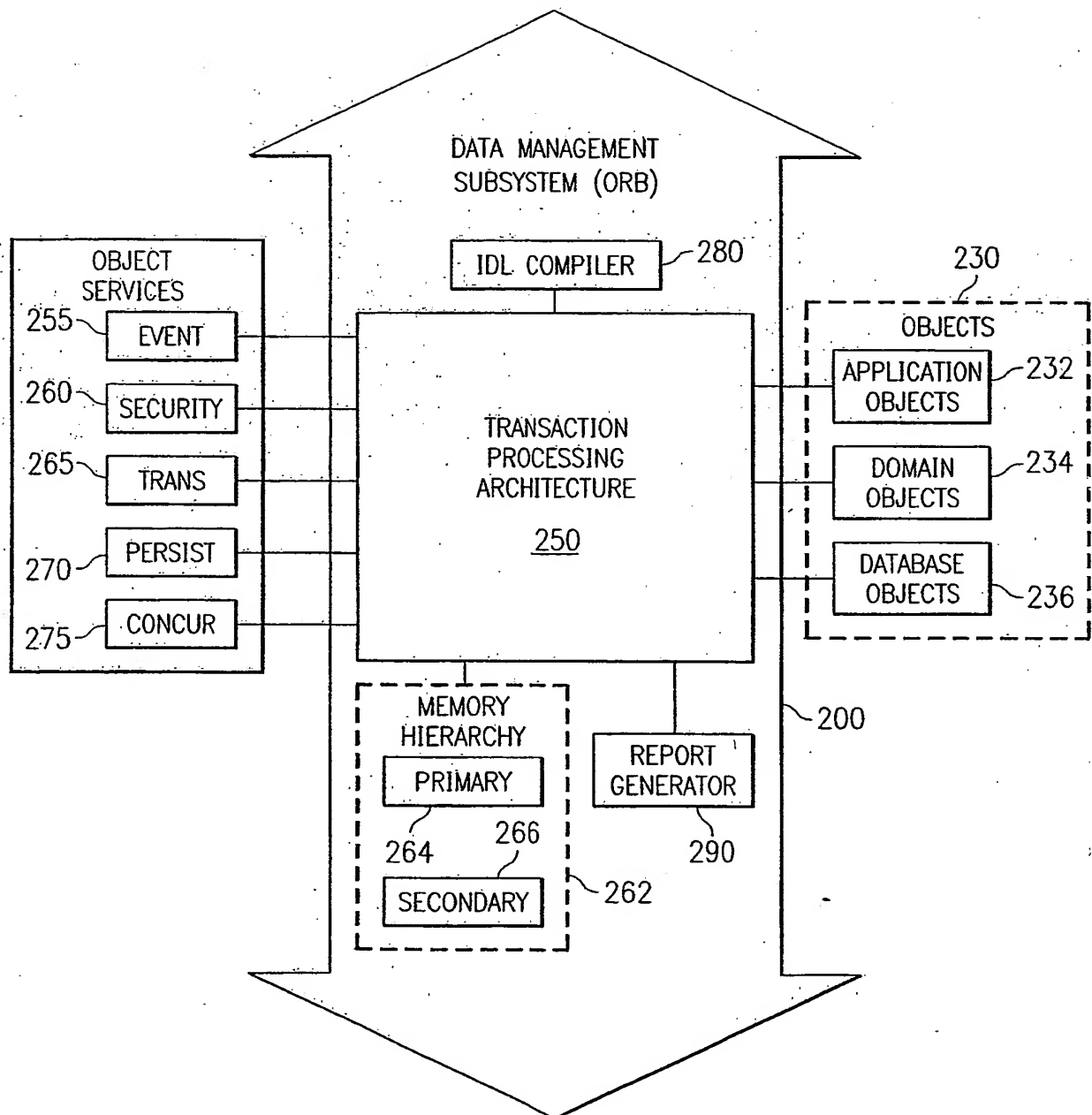


FIG. 2

3/7

FIG. 4



4/7

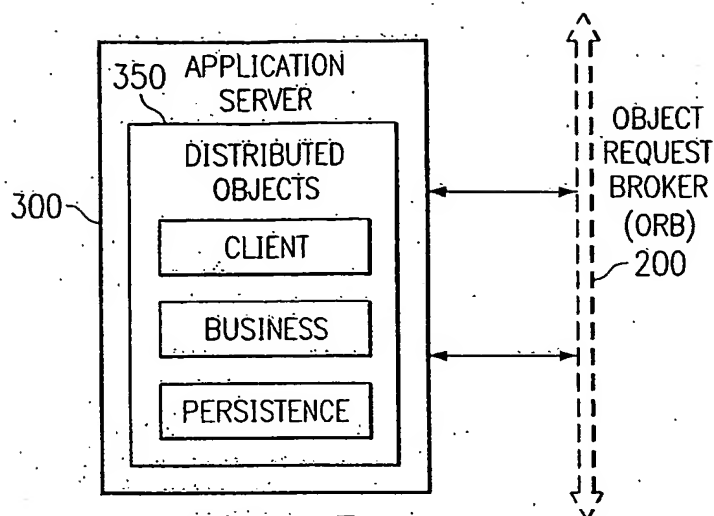


FIG. 5

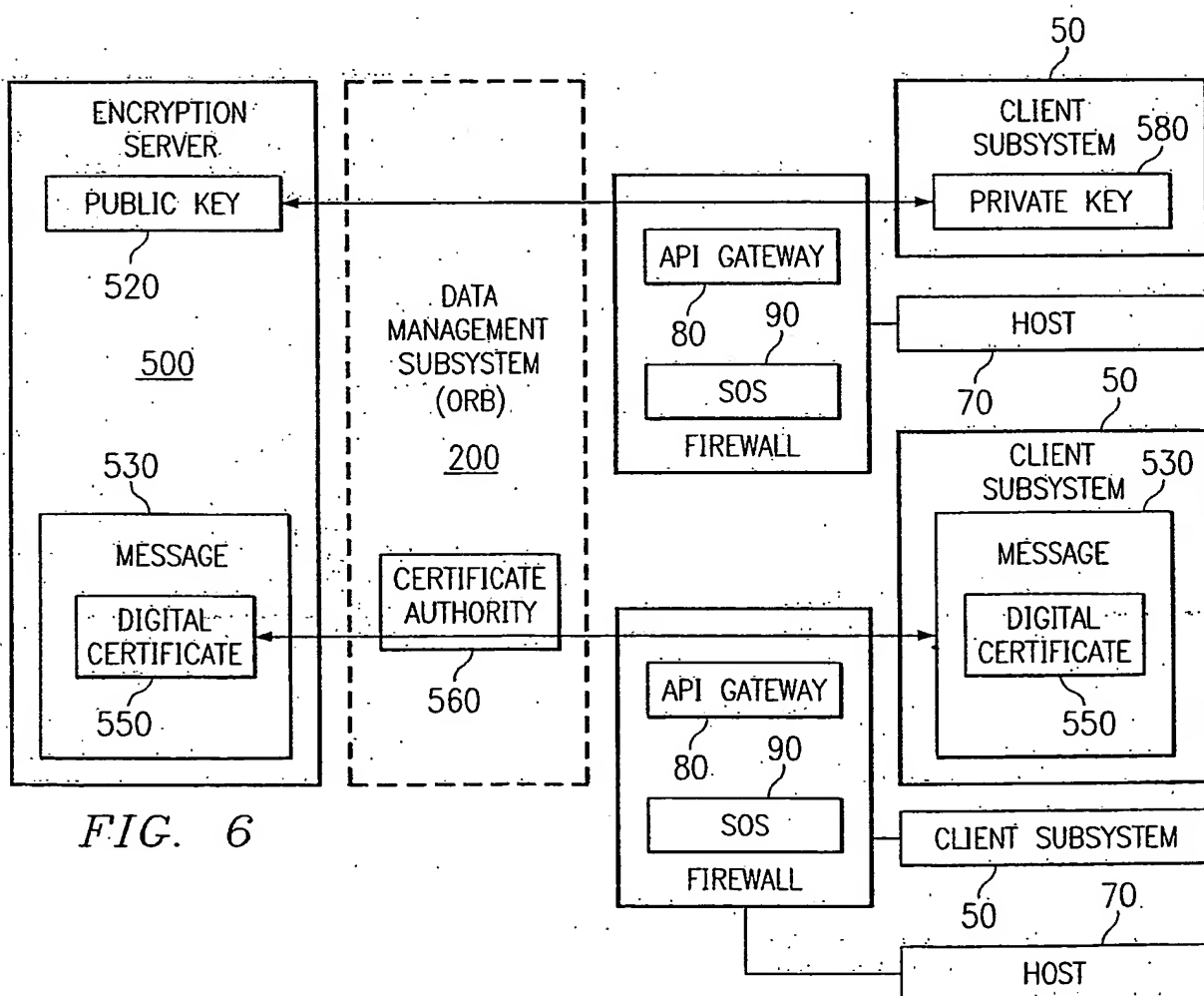


FIG. 6

5/7

FIG. 11

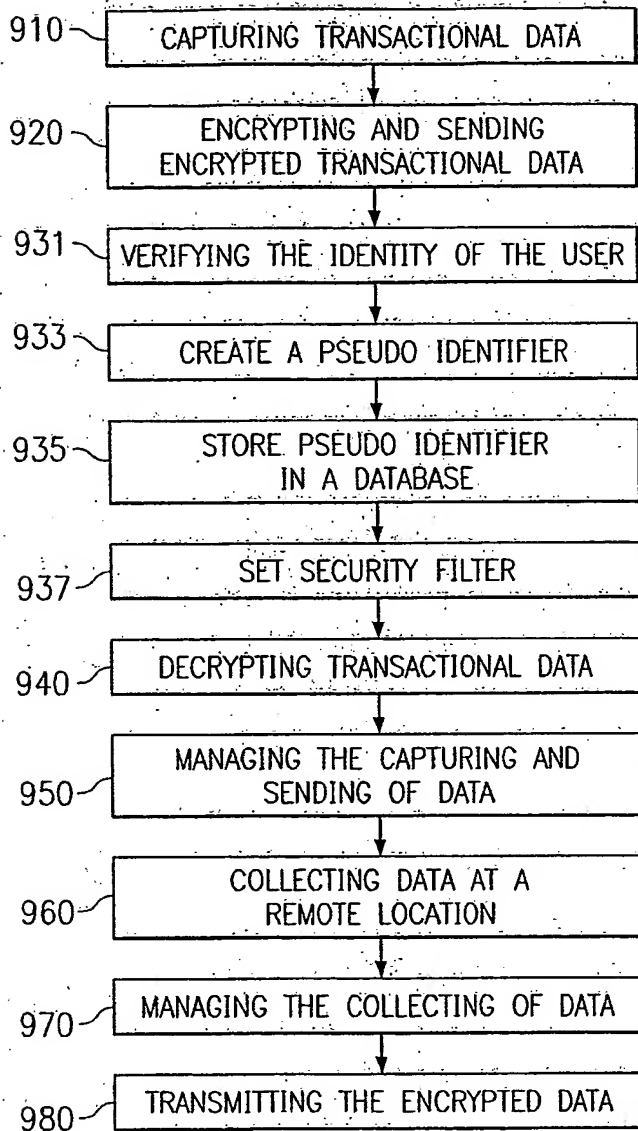
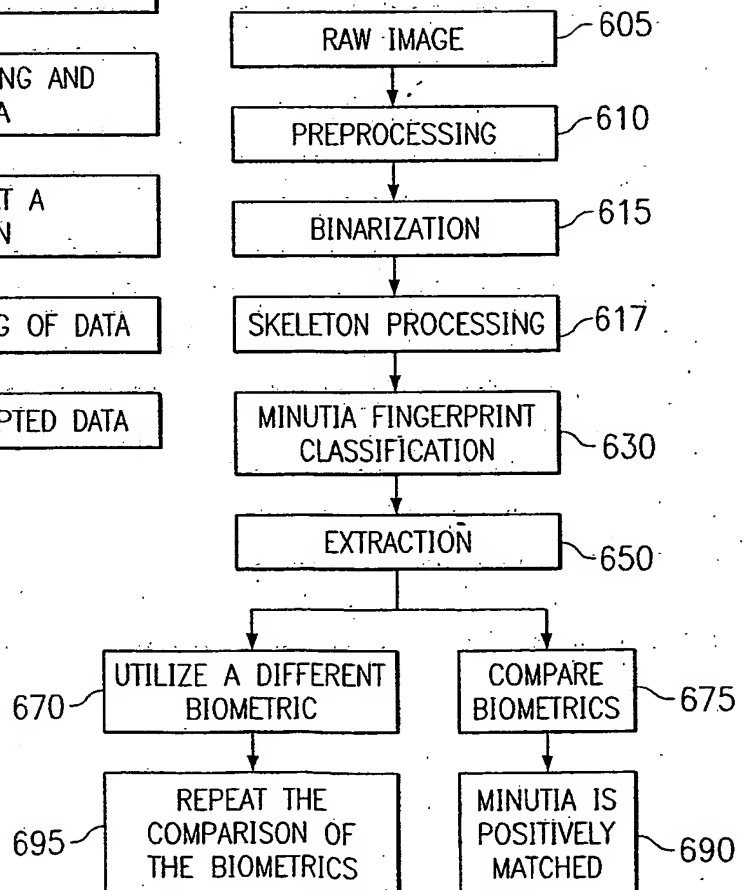


FIG. 7



6/7

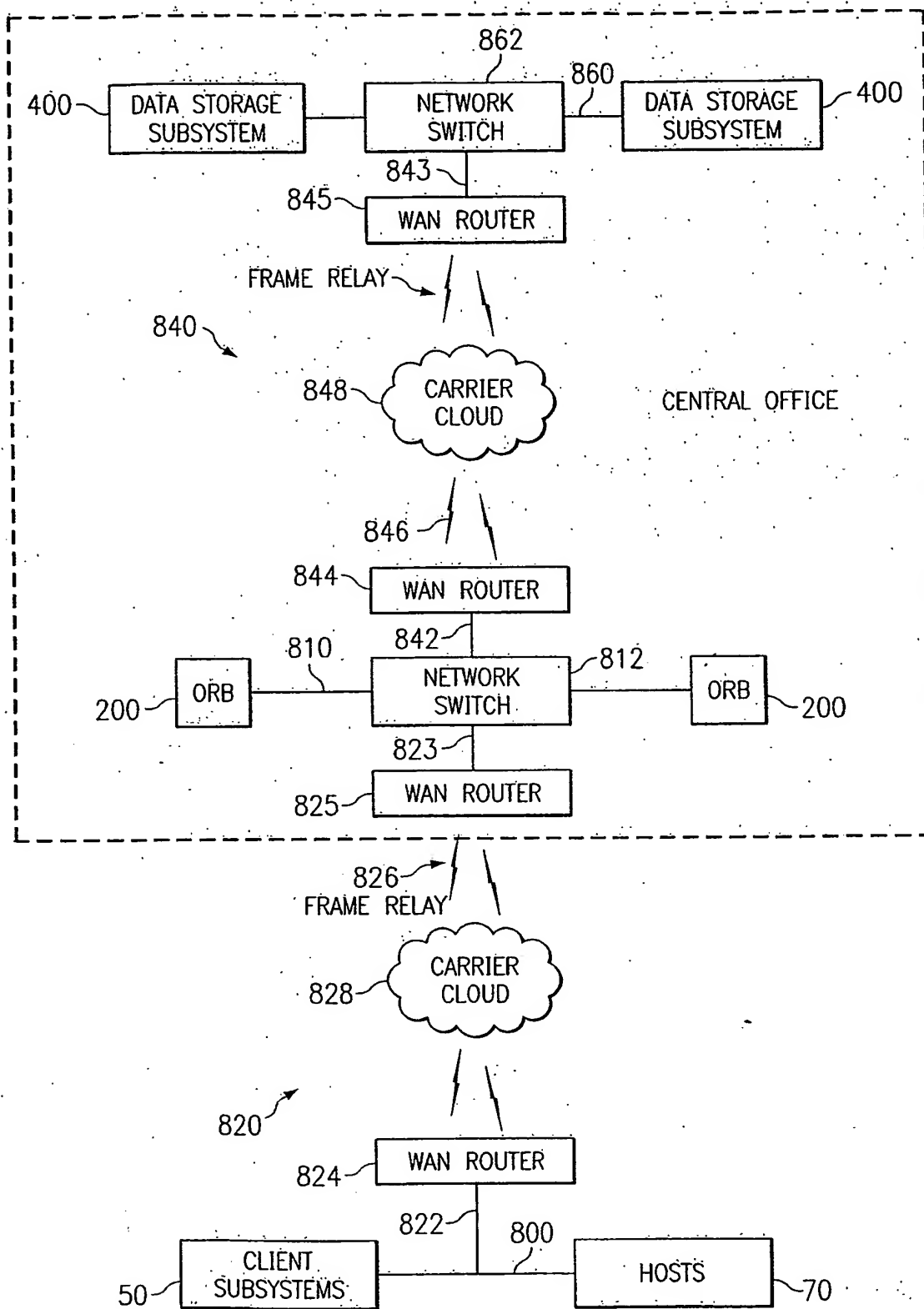


FIG. 8

7/7

FIG. 9

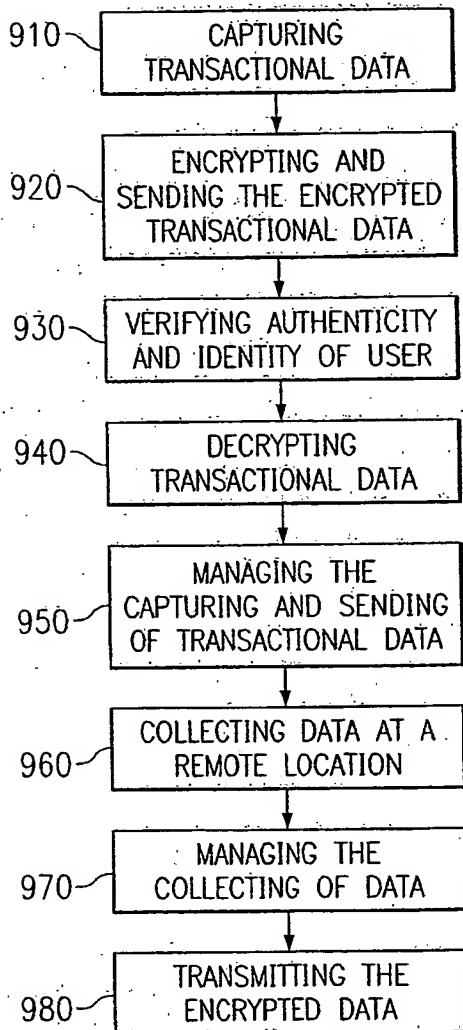
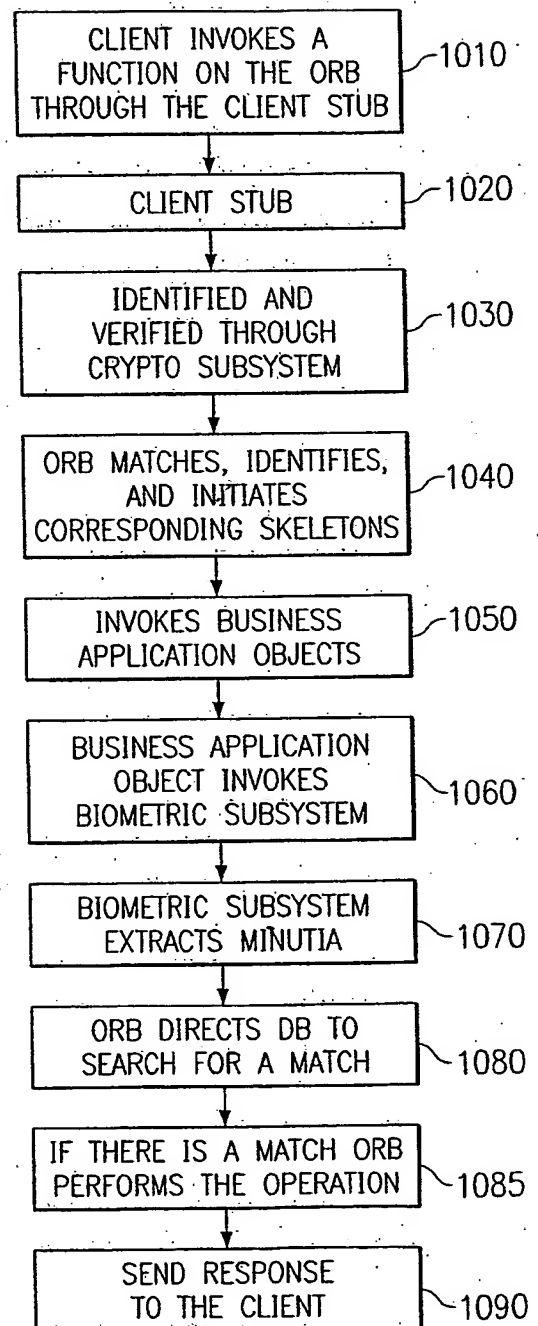


FIG. 10



(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
27 March 2003 (27.03.2003)

PCT

(10) International Publication Number
WO 2003/025718 A3

(51) International Patent Classification⁷: **G06F 1/00**,
21/00, H04L 29/06

(21) International Application Number:
PCT/GB2002/004228

(22) International Filing Date:
17 September 2002 (17.09.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/323,159 18 September 2001 (18.09.2001) US

(71) Applicant: **DATA TREASURY CORPORATION**
[US/US]; 175 Pinelawn Road, Suite 200, Melville, NY
11747 (US).

(71) Applicant (for MN only): **MAGGS, Michael, Norman**
[GB/GB]; Kiburn & Strode, 20 Red Lion Street, London
WC1R 4PJ (GB).

(72) Inventors: **BALLARD, Claudio R**; 16 West Neck Court
Lloyd Harbor, New York, NY 11743 (US). **PATHAK,**
Amirish; 7 Apple Blossom lane, East Patchogue, New

York, NY 11772 (US). **IMBRANCE, Michael T**; 291 East
Woodside Avenue, East Patchogue, New York, NY 11772
(US). **CURRIE, Edward H**; 6-57 158 Street, Whitestone,
New York, NY 11357 (US). **CASSATA, James**; 673
Meadow Road, Smithtown, New York, 11787 (US).

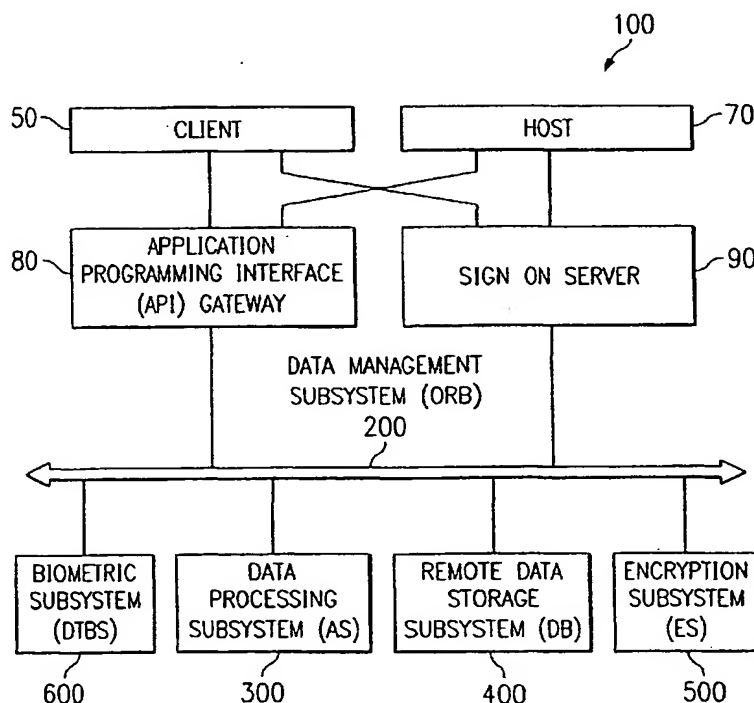
(74) Agents: **MAGGS, Michael, Norman**, et al.; Kilburn &
Strode, 20 Red Lion Street, London WC1R 4PJ (GB).

(81) Designated States (national): AE, AG, AL, AM, AT, AU,
AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU,
CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH,
GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC,
LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW,
MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG,
SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC,
VN, YU, ZA, ZM, ZW.

(84) Designated States (regional): ARIPO patent (GH, GM,
KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),
Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),
European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE,
ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK,
TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ,
GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: PRIVATE SECURE INFORMATION REPOSITORY WITH BIOMETRIC AUTHENTICATION



(57) Abstract: A system for remote data acquisition and private and secure and authenticated, centralized processing and storage is disclosed called the DataTreasury™ Repository System. The DataTreasury™ Repository System provides a secure system for the storage and retrieval of data comprising personal information, financial information, and general information. The identity of the users are held private through the use of a biometric as the sole personal identifier. The system acquires transactional data at least one remote locations, encrypts the data, transmits the encrypted data to a central location, transforms the data to a usable form, performs identification verification using biometric data, generates informative reports from the data and transmits the informative reports to the remote location(s), while maintaining privacy, security, and authenticity of the user's data and biometric. To ensure the complete security of the system, all data is re-encrypted while in storage, or when it is in a state of nonuse.

WO 2003/025718 A3



Published:

- with international search report
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(88) Date of publication of the international search report:

24 June 2004

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 02/04228

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00 G06F21/00 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 98/11750 A (SUBBIAH SUBRAMANIAN ; LI YANG (US); RAO D RAMESK K (US)) 19 March 1998 (1998-03-19) abstract claims 1,9,25,39,40,44; figures 1,2,4	1,2,45
X	US 5 838 812 A (PARE JR DAVID FERRIN ET AL) 17 November 1998 (1998-11-17) abstract; claims 1,14,16; examples 1-3	1,2,45
X	GB 2 354 612 A (NIPPON ELECTRIC CO) 28 March 2001 (2001-03-28) abstract; figures 4,3	1,2,45
P,X	EP 1 139 301 A (MATSUSHITA ELECTRIC IND CO LTD) 4 October 2001 (2001-10-04) paragraphs '0017!-'0033!,'0054!-'0060!; figures 2,3	1,2,45

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents:

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

T later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

X document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

Y document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

Z document member of the same patent family

Date of the actual completion of the international search

7 April 2004

Date of mailing of the international search report

19/04/2004

Name and mailing address of the ISA
European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Beker, H

INTERNATIONAL SEARCH REPORT

International Application No

PCT/GB 02/04228

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,X	WO 02/095552 A (IMPRIVATA INC) 28 November 2002 (2002-11-28) abstract; figures 1,3,5 -----	1,2,45
E	US 2002/174344 A1 (TING DAVID M T) 21 November 2002 (2002-11-21) paragraphs '0025!-'0036!; figures 1,2 -----	1,2,45

Continuation of Box I.2

Claims Nos.: 3-44,46-74

It was possible to search the claims 1,2,45 and find documents, namely the ones listed herein above, which relate to the subject claimed therein.

In fact, D1 = WO 98/11750, at the references in parentheses and in particular in its claims, discloses all the claimed features of those claims:

A system (Fig. 1) to provide a centralized, secured and authenticated storage of information comprising (claims 26 and 27 of D1):

- a) at least one client subsystem(102) to receive and send transactional data(claim 31, 39 items (a)) comprising:
 - i) at least one biometric processing client subsystem for capturing biometric data (101)
 - ii) at least one data capturing device(Fig. 4, 411) to capture any and all types of additional data;
- b) at least one remote data management subsystem (103) for managing the processing sending receiving, and storing of the transactional data (claim 39 item (a));
- c) at least one remote data storage subsystem to store any and all transactional data(Fig. 2, 107);
- d) at least one data processing subsystem for processing all transactional data, with the client subsystem providing encrypted subsystem identification information and encrypted transactional data to the data processing subsystem(claims 25, 44)
- e) at least one biometric subsystem to verify the user's identity(claim 25) and at least one encryption subsystem for ensuring the security of the transactional data; (claim 9) and
- f) at least one communication network (claim 9) for secure transmission of transactional data within and between said at least one client subsystem(102), and said at least one data management subsystem(103), wherein said at least one client subsystem further comprise at least one biometric device for capturing biometric data (Fig. 417).

However, the multitude of variations, modifications and combinations of these variations and modifications expressed in the multitude of dependent and independent claims renders the claims in their entirety so unclear and lacking conciseness, contrary to Art. 6 PCT, that a meaningful, complete search was not possible. Moreover, the description provides no unambiguous indication allowing to anticipate to which of this uncountable multitude of potential inventions the application might be directed to after amendment.

The applicant's attention is drawn to the fact that claims, or parts of claims, relating to inventions in respect of which no international search report has been established need not be the subject of an international preliminary examination (Rule 66.1(e) PCT). The applicant is advised that the EPO policy when acting as an International

Preliminary Examining Authority is normally not to carry out a preliminary examination on matter which has not been searched. This is the case irrespective of whether or not the claims are amended following receipt of the search report or during any Chapter II procedure.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/GB 02/04228

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☒ Claims Nos.: 3-44, 46-74
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:
see FURTHER INFORMATION sheet PCT/ISA/210
3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest.
- ☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International Application No

PCT/GB 02/04228

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
WO 9811750	A	19-03-1998	US 6219793 B1 AU 4341797 A EP 0931430 A2 WO 9811750 A2	17-04-2001 02-04-1998 28-07-1999 19-03-1998
US 5838812	A	17-11-1998	US 5613012 A US 5615277 A AT 254315 T AU 5922696 A BR 9608580 A CA 2221321 A1 CN 1191027 A DE 69630713 D1 DK 912959 T3 EP 0912959 A1 JP 11511882 T WO 9636934 A1 US 2002174067 A1 US 2002111917 A1 US 6366682 B1 US 6269348 B1 US 6230148 B1 US 2003105725 A1 US 6192142 B1 US 6012039 A US 6154879 A US 6397198 B1 US 2004020982 A1 US 5870723 A US 5764789 A US 2001000535 A1 US 5802199 A US 5805719 A US 2001029493 A1 US 2001039533 A1	18-03-1997 25-03-1997 15-11-2003 29-11-1996 05-01-1999 21-11-1996 19-08-1998 18-12-2003 15-03-2004 06-05-1999 12-10-1999 21-11-1996 21-11-2002 15-08-2002 02-04-2002 31-07-2001 08-05-2001 05-06-2003 20-02-2001 04-01-2000 28-11-2000 28-05-2002 05-02-2004 09-02-1999 09-06-1998 26-04-2001 01-09-1998 08-09-1998 11-10-2001 08-11-2001
GB 2354612	A	28-03-2001	JP 2000353204 A AU 3941200 A CN 1277400 A TW 476038 B	19-12-2000 14-12-2000 20-12-2000 11-02-2002
EP 1139301	A	04-10-2001	JP 2001273498 A CN 1328309 A EP 1139301 A2 US 2001026632 A1	05-10-2001 26-12-2001 04-10-2001 04-10-2001
WO 02095552	A	28-11-2002	WO 02095552 A2 WO 02095553 A2 WO 02095554 A2 WO 02095054 A2 US 2002174344 A1 US 2002174346 A1 US 2002174347 A1 US 2002174348 A1	28-11-2002 28-11-2002 28-11-2002 28-11-2002 21-11-2002 21-11-2002 21-11-2002 21-11-2002
US 2002174344	A1	21-11-2002	WO 02095552 A2 WO 02095553 A2 WO 02095554 A2	28-11-2002 28-11-2002 28-11-2002

INTERNATIONAL SEARCH REPORT

International Application No

PCT/GB -02/04228

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2002174344 A1		WO 02095054 A2	28-11-2002
		US 2002174346 A1	21-11-2002
		US 2002174347 A1	21-11-2002
		US 2002174348 A1	21-11-2002

This Page Blank (uspto)

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

This Page Blank (uspto)